Guida all'autodifesa digitale

- offline -

Contrabbandiera

0 | Prefazione

Scrivere una guida d'autodifesa digitale è un progetto ambizioso. Ci sono un mare di cose da dire, di dettagli a cui prestare attenzione, di responsabilità a cui non devi sottrarti. A volte corri il rischio di generare troppe paranoie, a volte troppo poche. Hai bisogno di precisione, di un certo grado di intransigenza, eppure anche di molta duttilità e capacità di immedesimazione.
Scrivere una guida d'autodifesa è un progetto ambizioso, perché spesso chi ti legge alla fin fine vorrebbe solo faticare il meno possibile. E non esiste ricetta, non esiste guida, non esiste manuale per chi ha troppa fretta e poca attenzione.
La Guide d'Autodefénse Numerique *può darsi che non sia perfetta, ma sicuramente ha un pregio che ce l'ha fatta stare a cuore: insegna un approccio lento e non pigro alla tecnologia. Il che, forse, è il primo vero buon consiglio. E il più importante.*
E chi siamo noi? Siamo alcune traduttrici che respirano insieme alla comunità italiana di Hackmeeting*, autogestiscono quanto più riescono del proprio giorno, amano le autoproduzioni e la condivisione dei saperi.*

0.1 Chi parla?

Purtroppo non abbiamo una risposta semplice da dare a questa domanda, ma ci piacerebbe dire lo stesso qualcosa. Innanzitutto ci teniamo alla possibilità di pubblicare un libro in modo anonimo, e questo per diverse ragioni.
Una di queste, che svilupperemo più avanti nel capitolo, è la domanda "qualcosa da nascondere?", a cui noi rispondiamo all'unisono: "sì!".

L'anonimato insomma è una maniera di proteggersi. Abbiamo poi scelto di non metterci in mostra individualmente, per spostare l'attenzione dal "chi" e lasciare invece sotto i riflettori il "cosa".
Inoltre, attraverso le varie fasi redazionali e le diverse pubblicazioni che si sono susseguite, il numero delle persone che ha partecipato, da vicino o da lontano, alla realizzazione di questa guida, ha fatto diventare ampio, in evoluzione e dai contorni indefiniti il collettivo che fa vivere questo progetto.
Infine, crediamo di aver lasciato abbastanza tracce in queste pagine per permettere a tutte le persone che ci leggono di collocarci, almeno parzialmente, all'interno dell'ambito dell'informatica, tecnica, politica o etica.
Ci sono due caratteristiche di quest'opera che ci obbligano a far fronte, per certi aspetti, alle domande relative alla sua provenienza. Questo lavoro ha la pretesa di trasmettere dei saperi e delle pratiche tecniche riservati normalmente a pochi specialisti. D'altro canto, la correttezza delle indicazioni fornite può avere delle conseguenze sulla serenità delle persone che le mettono in pratica. Piccoli errori in cui potremmo essere incappati potrebbero avere gravi ricadute.
È importante quindi spendere qualche parola su chi ha prestato la propria voce per questa guida. Mettere in chiaro la portata dei nostri saperi e ciò che sappiamo fare – compresi i nostri limiti – permette di trovare un rapporto di apprendimento più adeguato a questo scritto, ma anche di decidere il livello di fiducia *tecnica* che si merita. Quindi, collettivamente possiamo dire che:

- delle questioni sollevate da questa guida ci occupiamo, tecnicamente e politicamente, da una decina d'anni;
- conosciamo piuttosto bene il funzionamento di alcuni sistemi operativi, in particolare di quelli Debian GNU/Linux;

- abbiamo delle buone basi di crittografia, ma siamo molto lontani dal poter pretendere di dirci padroni dell'argomento;
- e per finire, affermiamo un'ultima volta che le parole dette in quest'opera, come tutte le parole di una guida, devono essere prese con delle pinze proporzionali alla posta in gioco.

0.2 Una guida?

Questa guida è un tentativo di mettere insieme e condividere quello che abbiamo imparato nel corso di anni di pratica, errori, riflessioni e discussioni. Nel contesto in cui viviamo, la sola via praticabile sembra quella di sapere immaginare e mettere in atto delle policy di sicurezza adatte.
Non solo le tecnologie evolvono molto velocemente, ma in queste pagine potremmo aver commesso degli errori o aver scritto cose che non sono (più) vere o che meriterebbero di essere riverificate spesso.
Cercheremo quindi di aggiornare queste annotazioni agli indirizzi *https://guide.boum.org/* (versione francese) e *https://numerique.noblogs.org/* (versione italiana). L'intento che sta dietro alla guida è quello di fornire mappe, sestante e bussola a chiunque voglia intraprendere questo cammino. Da leggere, rileggere, praticare in solitaria o in più persone, da far scoprire e condividere. Per affinare l'arte della navigazione nelle torbide acque del mondo digitale.
Per rendere il tutto più digeribile, e data la mole di materiale prodotto, abbiamo diviso tutto quello che volevamo raccontare in due tomi (*Offline / Online*). A seconda che ci si trovi con un solo computer o se quest'ultimo è invece connesso a una rete, ci troviamo in contesti differenti, con minacce, bisogni e risposte diverse.

0.3 L'altro lato della memoria digitale

Oggi i computer, internet e i telefoni cellulari tendono a prendere sempre più spazio nelle nostre vite. Il digitale sembra spesso molto pratico: è rapido, si può parlare con un sacco di gente molto lontana, si può avere tutta la nostra storia espressa in foto, si possono scrivere facilmente dei testi ben formattati... Ma tutto questo non comporta solo vantaggi; o perlomeno, questi vantaggi non sono solo a nostra disposizione, ma anche di altre persone che possono non essere necessariamente benevole.
In effetti è molto più facile ascoltare discretamente delle conversazioni attraverso i telefoni cellulari piuttosto che in mezzo a una strada rumorosa, o trovare delle informazioni all'interno di un hard-disk piuttosto che in uno scaffale strabordante di carte.
Inoltre un'enorme parte dei nostri dati personali finisce per essere pubblicata da qualche parte, da noi stessi o da altre persone, perché ci incitano a farlo – è un po' il tema di fondo del web 2.0 commerciale – perché sono le stesse tecnologie a lasciare tracce o semplicemente perché non facciamo attenzione.

0.4 Niente da nascondere?

"Basta essere paranoici: io non ho niente da nascondere!" si potrebbe rispondere alla considerazione precedente. Ma riguardo a questo ci sono due esempi che, in modo molto semplice, tendono tuttavia a dimostrare il contrario: nessuno vorrebbe vedere i propri codici della carta di credito o dell'account Amazon finire nelle mani di qualcun altro; e a nessuno piacerebbe farsi svaligiare la casa perché il proprio indirizzo è stato a sua insaputa pubblicato su internet e il fatto che pro-

prio in quel momento non era in casa era stato confermato sui social network.
Ma al di là di queste futili questioni di difesa della proprietà privata, la riservatezza dei dati dovrebbe essere un fatto interessante *di per se stesso*.
Innanzitutto perché non siamo noi a decidere chi è autorizzato o no a fare cosa con un computer. C'è chi viene arrestato sulla base di tracce lasciate attraverso l'utilizzo di strumenti digitali nel quadro di attività che non piacciono a un governo (non necessariamente il proprio), e non succede solamente in Cina o in Iran.
In molti, governanti, datori di lavoro, pubblicitari, guardie & malintenzionati, hanno interesse a ottenere l'accesso ai nostri dati. Il crescente posto che prende l'informazione nell'economia e nella politica mondiale non può che incoraggiarli.
Sappiamo già da soli che non si fanno problemi a tracciare le intersezioni tra gli individui. Cosa sappiamo delle pratiche, legali e illegali, attuate su chi ci sta vicino?
Inoltre, come sapere se chi è autorizzato oggi lo sarà anche domani? I governi cambiano, le leggi e le situazioni anche. E le cose possono andare estremamente veloci, come hanno potuto constatare in molti, dal 2015, con l'applicazione dello Stato d'Emergenza in Francia. Se non abbiamo niente da nascondere oggi, per esempio la frequentazione abituale di un sito web militante, come sappiamo che quello stesso sito non si ritroverà legato a un processo repressivo in futuro? *Verranno lasciate varie tracce sul computer* e potranno essere impiegate come elementi di prova.
Mettere in atto delle pratiche di protezione dei dati anche quando si sente di non averne direttamente bisogno permette di renderle più "normali", più accettabili e meno sospette. Le persone che non hanno altra possibilità di sopravvivenza se non quella di nascondere le proprie attività digitali ce ne saranno riconoscenti, senza alcun dubbio.

Generalmente, tendiamo a contenere le nostre azioni quando sappiamo che altri possono ascoltarci, guardarci o leggerci: canteremmo sotto la doccia se sapessimo che abbiamo delle microspie installate? Ci metteremmo a imparare a ballare se delle telecamere fossero puntate su di noi? Scriveremmo una lettera privata così liberamente se ci fosse una persona dietro le nostre spalle a leggere? Avere delle cose da nascondere non è soltanto una questione di legalità, ma anche di *intimità*.
E così, nell'epoca delle società con un controllo sempre più paranoico, sempre più decise a scovare la sovversione e a vedere dietro a ciascun essere umano un potenziale terrorista che va sorvegliato da vicino, nascondersi diventa un interesse *politico* e, di fatto, *collettivo*. Non fosse altro che per mettere i bastoni tra le ruote di coloro che ci vogliono trasparenti e reperibili in ogni momento.
Tutto ciò può portarci a dire che non abbiamo alcuna voglia di essere controllabili da qualche Grande Fratello che sia già esistente o del quale stiamo profetizzando la venuta. La cosa migliore è senza dubbio quella di impedire che tutti questi meravigliosi strumenti che le tecnologie moderne ci offrono (e offrono anche al Grande Fratello) ci si rivoltino contro.
Insomma, dobbiamo avere anche noi qualcosa da nascondere, *se non altro per confondere le tracce*!

0.5 Comprendere per poter scegliere

Questa guida vuole provare a descrivere in termini comprensibili l'intimità – o piuttosto la sua assenza – nel mondo digitale. Si tratta di chiarimenti su alcuni concetti che ci sono stati dati, per capire meglio ciò a cui ci esponiamo con l'utilizzo di strumenti che non sono neutri. Ma vuole anche offrire un ventaglio di possibili "soluzioni", mai inoffensive se non ci si rende conto di ciò da cui non sono in grado di proteggerci.

Attraverso la lettura di queste pagine, si potrebbe arrivare a pensare che niente è veramente sicuro con un computer: ebbene sì, è vero. Ed è anche falso. Esistono degli strumenti e degli utilizzi appropriati. E spesso la questione alla fine non è tanto se utilizzare o no queste tecnologie, ma piuttosto quando e come utilizzarle (o non utilizzarle).

0.6 Prendersi il tempo per capire

I software semplici da utilizzare muoiono dalla voglia di sostituirsi al nostro cervello. Se da una parte ci consentono un utilizzo facile dell'informatica, dall'altra ci privano anche delle decisioni sui frammenti di vita che gli affidiamo.
Con l'accelerazione dei computer e delle nostre connessioni a internet, è arrivato il regno dell'istantaneità. Grazie al cellulare e al wi-fi, il gesto di riattaccare il telefono o di collegare un cavo di rete al proprio computer per comunicare è già qualcosa di desueto.
Avere pazienza, prendersi il tempo per imparare o riflettere è diventato superfluo: vogliamo tutto, subito, vogliamo la soluzione. Ma questo implica il confidare nelle molte decisioni prese da esperti distanti ai quali crediamo sulla parola. Questa guida ha come scopo quello di proporre altre soluzioni, che necessitano di prendersi il tempo per capirle e applicarle.
Adattare le proprie pratiche all'utilizzo che si ha del mondo digitale è quindi necessario nel momento in cui vogliamo, o dobbiamo, avere una certa attenzione al suo impatto. Ma l'impresa non ha molto senso se è solitaria. Vi sproniamo quindi a costruirvi una zattera digitale, saltarci gioiosamente a bordo, senza dimenticare di portarvi dietro questa guida e qualche razzo di soccorso per inviarci le vostre osservazioni a *guide@boum.org* (in francese o inglese) o a *if_do@autistici.org* (italiano).

0.7 Ultimi aggiornamenti e revisioni

Meno di un anno dopo la pubblicazione dell'ultima edizione online della guida, ci siamo apprestati a prepararne un'altra, sia per offrire una nuova edizione cartacea sia per seguire l'evoluzione dei software che avevamo raccomandato nelle precedenti, ma anche a causa dei mutamenti nella situazione politica francese.

Qualche mese dopo la più grande fuga di documenti confidenziali della CIA, la creazione di uno Stato d'Emergenza in Francia ha confermato la tendenza politica verso una vera e propria normalizzazione della sorveglianza. Una tendenza che il rilascio dei documenti segreti della NSA da parte di Edward Snowden aveva già anticipato. In effetti, l'armamentario di software di sorveglianza o di infiltrazione elettronica extra-legale venuto a galla man mano insieme agli scandali è stato fatto rientrare zitto zitto nell'arsenale legislativo. E, quando serve, il fine giustifica i mezzi e viene permesso agli agenti governativi di utilizzare questi strumenti senza scrupoli e senza rischio di scandalizzare l'opinione pubblica.

La magra consolazione che possiamo trarre da questo nuovo contesto è che sappiamo con più chiarezza da cosa dobbiamo proteggerci. Ma questo rilancia anche la palla alla sicurezza informatica, obbligando "gli attaccanti" a ricorrere a tecniche ancora più potenti, come l'utilizzo di falle informatiche ancora sconosciute al pubblico contro le quali è difficile trovare rimedio. Vulnerabilità che vengono chiamate "Zero Day". Una vulnerabilità di questo tipo è stata per esempio utilizzata dall'FBI nel 2015 durante l'operazione *Pacifier*, un'altra simile è quella del caso *Ransomware Wannacry* che ha coinvolto più di trentamila computer di tutto il mondo nella primavera del 2017.

Sul piano legale, in Francia, ci sono state almeno quattro nuove leggi riguardanti la sorveglianza informatica e di internet:

la Legge di rinforzo ai dispositivi relativi alla lotta contro il terrorismo, la Legge relativa all'informazione, la Legge in materia di misure di sorveglianza delle comunicazioni elettroniche internazionali e infine la Legge di rinforzo alla lotta contro il crimine organizzato, il terrorismo e il loro finanziamento. Quest'ultima legge autorizza per esempio le guardie a installare da remoto dei captatori, quando si trovano all'interno di un'inchiesta che riguarda una lista di reati talmente lunga da poterci far rientrare quello che gli conviene. Inoltre lo Stato d'Emergenza ha permesso di ampliare il loro raggio d'azione in modo da concedergli di agire senza l'avvallo di un giudice, in particolare permettendo il sequestro di materiale informatico durante una perquisizione amministrativa, ovvero senza l'autorizzazione di un giudice.
Insomma, la protezione dell'intimità e della libertà d'espressione su internet sono più che mai d'attualità.
Per ciò che riguarda internet, un esempio evidente è la criminalizzazione della consultazione "abituale" dei siti web "che fanno apologia di terrorismo", cosa che ha già mandato in prigione due persone: il primo si definiva un "apprendista giornalista"[1] mentre il secondo ha detto di agire per curiosità[2]. I due si sono beccati due anni di prigione. Questo reato è stato depenalizzato dal Consiglio Costituzionale all'inizio di febbraio 2017, ma reintrodotto soltanto18 giorni più tardi.
Diverse persone sono state condannate per la pubblicazione di articoli, accusati di fare "apologia di terrorismo". Il rapporto *Freedom of the net* del 2015 riporta che "a Nantes un sedicenne è stato arrestato per aver condiviso su Facebook una vignetta legata all'attacco di Charlie Hebdo. La caricatura in questione prendeva in giro la copertina di luglio 2013 di Charlie Hebdo, pubblicata dopo il massacro di centinaia di egiziani che manifestavano contro il vecchio presidente isla-

---

1 http://nbl.gs/qgf
2 http://nbl.gs/qgg

mista Mohamed Morsi, e rappresentava un uomo musulmano che reggeva il Corano per proteggersi dai proiettili e sopra c'era scritto "questo non ferma i proiettili". L'artista Dedko ha sostituito il corano con il giornale di Charlie Hebdo e l'uomo musulmano con uno dei suoi disegnatori. Diverse voci hanno accusato le autorità francesi di usare due pesi e due misure per i casi di libertà di espressione[3].

Gli scenari più allarmisti purtroppo sono divenuti pane quotidiano in materia di sorveglianza elettronica. Malgrado la diffusione di un sentimento d'impotenza, queste differenti rivelazioni sullo stato generale della sorveglianza digitale, rendono ancora più necessario dotarsi di strumenti in grado di farne fronte.

Riguardo ai software, il mese di giugno 2017 ha visto l'uscita della nuova versione di Debian, battezzata Stretch, e anche la versione 3.0 del sistema Live Tails, d'ora in avanti basato su Stretch. Questo aggiornamento ha portato numerosi cambiamenti tanto a livello grafico, quanto nei software proposti. Abbiamo dunque dovuto rivedere le cose per correggere gli "howto" su questi nuovi sistemi. Questo ha portato all'aggiunta del programma OnionShare e all'arricchimento del programma OpenPGP con la cifratura e decifratura dei documenti.

Grazie a questa revisione, speriamo che le pagine che seguono vi siano d'aiuto durante la vostra traversata della giungla digitale... almeno fino al prossimo aggiornamento.

---

3 http://nbl.gs/qgi

PRIMA PARTE

Comprendere

Di fronte alla grande complessità degli strumenti informatici e numerici, la quantità di informazioni da ingurgitare per tentare di acquisire qualche pratica di autodifesa può apparire enorme. Lo è sicuramente per chi cerca di capire tutto quanto insieme.
Questo primo tomo si concentra quindi sull'utilizzo di un computer offline – o, per meglio dire, prima di connetterlo a qualunque cosa. Ci sono delle conoscenze più generali che valgono nel caso in cui il computer sia connesso o no a una rete. Mettiamo quindi da parte, per adesso, le minacce specificatamente legate all'uso di internet e delle risorse web.
Su questa parte offline ci prenderemo il tempo di attardarci su alcune questioni di base, le loro implicazioni in termini di sicurezza / fiducia / intimità[1]. Dopo aver analizzato alcuni casi concreti di impiego, potremo esaminare alcune ricette pratiche.
Un'ultima precisazione prima di buttarci: *l'illusione di sicurezza è molto peggio della consapevolezza netta di una vulnerabilità.* Quindi, prendiamoci il tempo di leggere bene queste parti introduttive prima di gettarci sulle nostre tastiere... o di gettare i nostri computer dalla finestra.

---

1 Intendiamo qui riferirci a una nozione un po' imprecisa: qualcosa che riguarda la possibilità di decidere cosa rivelare a chi e cosa invece tenere segreto; qualcosa che include anche una certa attenzione nell'ostacolare i tentativi di violare questi segreti. Il termine impiegato in inglese per definire ciò di cui parliamo qui è *privacy*. Nessuna parola italiana ci è sembrata adatta per includere tutti i sensi che vorremmo intendere con questo termine. Altrove incontreremo spesso il termine "sicurezza", ma l'utilizzo che ne viene fatto comunemente ci ha fatto venire voglia di evitarlo.

1 | Informazioni di base su un computer

Cominciamo dall'inizio.
Un computer non è un cappello magico in cui si possano infilare e togliere conigli quando se ne ha bisogno, o che ci permette di avere una finestra aperta sull'altro capo del mondo premendo il tasto giusto.
Un computer è un insieme di macchine più o meno complesse, collegate tra loro da connessioni elettriche, cavi e a volte onde radio. Tutto questo materiale accumula, trasforma e replica dei segnali per manipolare l'informazione che poi vediamo su un bello schermo pieno di bottoni da cliccare.
Capire come si articolano questi principali componenti, comprendere le basi di quello che li fa funzionare, è il primo passo per capire quali sono i punti forza e i punti deboli di queste macchine a cui affidiamo un buon numero dei nostri dati.

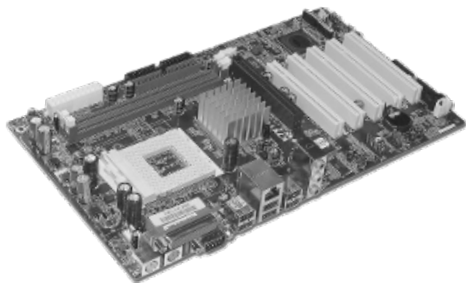
1.1 Macchine che trattano dati

I computer sono delle macchine inventate per occuparsi delle informazioni. Sanno quindi registrare, trattare, analizzare e classificare con precisione informazioni, anche in grande quantità.
Nel mondo digitale, copiare un'informazione "costa" solo qualche micro-watt, ovvero poca cosa: questo è importante capirlo se vogliamo limitare l'accesso a delle informazioni.
Bisogna molto semplicemente considerare che *mettere un'informazione su un computer* (ed è ancora più vero quando esso è in rete), *vuol dire accettare che questa informazione possa sfuggirci di mano.*
Questa guida può aiutare a limitare il danno, ma bisogna malgrado tutto prendere atto di questa realtà.

1.2 Il materiale

Somma di componenti collegati tra loro, il nostro computer è quindi innanzitutto un accumulo di oggetti che possiamo toccare, spostare, moddare, rompere.
L'insieme di schermo / tastiera / case, o il computer portatile, è pratico quando vogliamo semplicemente collegare i cavi al posto giusto. Ma per sapere cosa accade ai nostri dati è necessario un esame più raffinato.
Qui di seguito prendiamo in esame il contenuto di un computer "classico", talvolta chiamato pc. Ma troveremo la maggior parte di questi componenti, con delle leggere variazioni, su altre macchine: telefoni cellulari, modem, tablet, lettori mp3, registratori di cassa, contatori dell'energia elettrica, centraline digitali delle automobili, ecc.

1.2.1 La scheda madre

Un computer è composto più che altro da componenti elettronici. La scheda madre è un grosso circuito stampato che permette di collegare la maggior parte di questi componenti attraverso l'equivalente di fili elettrici. Sulla scheda madre

vengono attaccati almeno un processore, della RAM, un dispositivo di stoccaggio (hard-disk o un altro tipo di memoria), ciò che fa avviare il computer (il firmware), altre schede e periferiche, a seconda dei bisogni.
Andiamo a fare rapidamente un piccolo tour attraverso tutto questo per avere una vaga idea di chi fa cosa: ci sarà utile per il futuro.

1.2.2 Il processore

Il processore, chiamato anche CPU (Central Processing Unit o Unità di Elaborazione Centrale, in italiano) è il componente che si occupa del trattamento dei dati.
Per immaginarsi il lavoro di un processore, l'esempio più concreto sul quale basarsi è la calcolatrice: in una calcolatrice si inseriscono dati (i numeri) e delle operazioni da fare (somma, moltiplicazione o altre) poi si osserva il risultato, utile eventualmente in seguito come base per altri calcoli.
Un processore funziona esattamente alla stessa maniera. A partire da alcuni dati (che possono essere una lista di operazioni da effettuare), esso esegue semplicemente la catena di procedure da fare. Fa solo questo, ma lo fa velocemente.
Ma se il processore non è altro che una semplice calcolatrice, com'è possibile che riesca a eseguire delle operazioni su delle informazioni che non sono numeri, per esempio su un testo, delle immagini, dei suoni o lo spostamento del mouse?
Semplicemente trasformando in numeri tutto ciò che non lo è, utilizzando un codice definito in precedenza. Per un testo, potrebbe essere ad esempio una cosa tipo: `A = 65`, `B = 66`, ecc. Una volta che si è definito questo codice, si possono far diventare numeri le nostre informazioni. Usando il codice di prima possiamo per esempio trasformare "`GUIDA`" in "`71`, `85`, `73`, `44`, `65`".

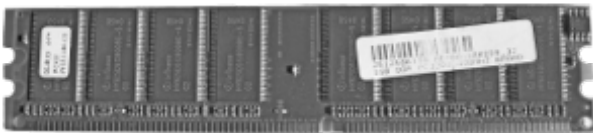
Questa serie di cifre permette di rappresentare le lettere che compongono le nostre parole. Ma il processo di digitalizzazione perderà sempre delle informazioni. Nell'esempio di prima, nel passaggio si perde la specificità della scrittura manoscritta dove per esempio una cancellatura, delle lettere esitanti, fanno parte anch'esse dell'"informazione". Quando le cose passano al setaccio del mondo digitale, nel passaggio si perdono per forza ogni volta dei pezzi.

Al di là dei dati, le operazioni che il processore deve effettuare (le sue istruzioni) sono anch'esse codificate sotto forma di numeri binari. Un programma è insomma una serie di istruzioni, trattate come qualsiasi altro dato.

> All'interno del computer, tutti questi numeri sono a loro volta rappresentati usando gli stati elettrici: assenza di corrente o presenza di corrente. Ci sono quindi due possibilità: i famosi 0 e 1 che troviamo ovunque. Questo è il motivo per cui si parla di codice binario, dove l'unità di misura è il bit. Ed è soltanto attraverso un gomitolo di cavi e diversi miliardi di transistor (interruttori, non molto diversi da quelli che accendono e spengono la luce in cucina) che si compie il trattamento dei dati.

I processori non funzionano tutti allo stesso modo. Alcuni sono stati progettati per essere più efficaci con certi tipi di calcolo, altri per consumare meno energia, ecc. Inoltre non tutti i processori dispongono esattamente delle stesse istruzioni. Ne esistono diverse grandi famiglie, che vengono chiamate architetture. Questo è abbastanza importante, perché un programma previsto per funzionare su una certa architettura generalmente non funzionerà su un'altra.

1.2.3 La RAM

La memoria, o RAM (Random Access Memory), si presenta spesso sotto forma di barrette, e si innesta direttamente sulla scheda madre.
La memoria serve ad archiviare tutti i programmi e i documenti aperti. È qui che il processore va a cercare i dati da trattare e a immagazzinare i risultati delle operazioni. Per effettuare i calcoli, queste informazioni devono quindi per forza trovarsi in una forma utilizzabile direttamente.
L'accesso alla RAM è molto rapido: il tempo necessario a girare gli interruttori che collegano il processore alla zona di memoria da leggere (o da scrivere).
Quando la RAM non è più alimentata dall'elettricità, i dati che essa conteneva diventano illeggibili entro pochi minuti o ore, secondo i modelli.

1.2.4 L'hard-disk

Dato che la RAM si dissolve quando non ha più corrente, il computer ha bisogno di un altro posto dove archiviare dati e programmi tra un'accensione e l'altra. Si parla anche di memoria "persistente" o memoria "secondaria": una memoria dove le informazioni scritte rimangono anche senza alimentazione elettrica.
Per fare ciò si utilizza in genere un hard-disk. Spesso questo è costituito da un involucro di metallo nel quale si trovano alcuni dischi che girano senza sosta. Sopra questi dischi si trovano dei piccolissimi pezzi di ferro. Al di sopra di ciascun disco stanno delle testine di lettura. Con l'aiuto dei campi magnetici, queste ultime individuano e modificano la posizione dei pezzetti di ferro. La posizione del pezzetto di ferro permette di codificare le informazioni da archiviare. Queste informazio-

ni sono immagazzinate sotto forma di bit, di cui esistono varie unità di misura, che permettono di quantificare più semplicemente la capacità di un hard-disk in termini di megabyte (MB), gigabyte (GB), ecc.
A causa dei movimenti meccanici, gli hard-disk che girano sono lenti. Questo spiega come mai, nel 2016, più di un terzo dei computer portatili nuovi conteneva un disco SSD invece di un hard-disk. Un disco SSD è infatti una memoria flash, la stessa presente nelle penne USB e nelle schede SD. Que-

sta memoria interamente elettronica è molto più rapida degli hard-disk magnetici (circa 25 volte più rapida).
Sia gli hard-disk che i dischi SSD permettono di conservare molte più informazioni rispetto alla RAM.
Le informazioni che si mettono quindi in genere su un disco (hard-disk o SSD) sono, ovviamente, i documenti, ma anche i programmi e tutti i dati che questi ultimi utilizzano per funzionare, come i file temporanei, i log, i file di salvataggio, i file di configurazione, ecc.
Il disco conserva insomma una memoria semi-permanente e semi-esaustiva di tutti i tipi di tracce che parlano di noi, di ciò che facciamo, con chi e come, da quando abbiamo iniziato a utilizzare il computer.

1.2.5 Le altre periferiche

Già soltanto con un processore, della RAM e un supporto di archiviazione, si è in grado di ottenere un computer. Non molto fruibile, però. Quindi gli si aggiungono generalmente altre periferiche come una tastiera, un mouse, uno schermo, una scheda di rete (con o senza fili), un lettore DVD, ecc.
Alcune periferiche necessitano di *bus*[2] supplementari per fare in modo che il processore possa accedervi. Questi bus possono essere saldati direttamente sul circuito della scheda madre (tipicamente nel caso della tastiera) o talvolta possono aver bisogno di un circuito supplementare, sotto forma di scheda.
Per ridurre il numero di bus specifici (quindi costosi e complicati da mettere a punto), i sistemi di accesso alle periferiche tendono a uniformarsi. Per esempio, lo standard USB (Universal Serial Bus) è diventato velocemente lo standard per con-

---

2 Il bus è, in informatica, un canale di comunicazione (tipicamente composto da cavi o da piste di circuiti stampati) che permette a differenti componenti hardware di scambiarsi informazioni [NdT].

nettere stampanti, tastiere, mouse, hard-disk esterni, schede di rete o quelle che chiamiamo in genere “penne USB”.

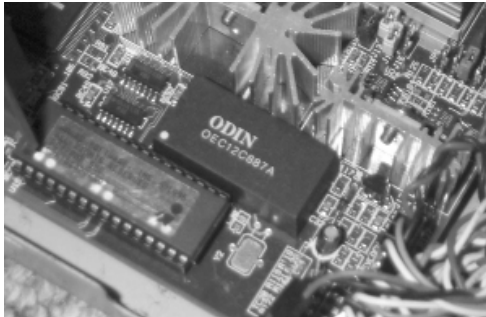
1.2.6 Il firmware della scheda madre

Per far funzionare il computer, bisogna fornire al processore un primo programma in grado di caricare a sua volta i programmi da eseguire in seguito.
Questo piccolo software, chiamato firmware della scheda madre, è contenuto in un chip di memoria fissato sulla scheda madre stessa. Questa fa parte di una terza tipologia di memorie: le memorie flash. Lo stesso tipo che troviamo nelle penne USB o negli hard-disk chiamati SSD (*Solid State Drive*). È una memoria che conserva le informazioni finché è attiva, ma se ne può sovrascrivere il contenuto attraverso un’operazione chiamata “flash”.
Il firmware storico per la maggior parte dei Personal Computer è stato chiamato BIOS (Basic Input/Output System). Dal 2012 in poi sempre più computer utilizzano un nuovo standard chiamato UEFI (Unified Extended Firmware Interface).
Questo primo programma che esegue il computer permette, tra l’altro, di scegliere dove si trova il sistema operativo[3] da utilizzare (che sarà caricato a partire da un hard-disk, da una penna USB, da un CD o un DVD, oppure dalla rete).

1.3 Elettricità, campi magnetici, rumore e onde radio

Dopo questo rapido tour all’interno dei suoi componenti, occorre prendere atto di diverse cose, per quanto riguarda la

3 Cap. 1.4.1

riservatezza delle informazioni che transitano dentro a un computer; prima di tutto, che la parte essenziale delle informazioni circola sotto forma di corrente elettrica. Quindi niente impedisce di poter mettere l'equivalente di un banale voltmetro per misurare la corrente che passa, e ricostruire poi i dati manipolati dal computer in una forma o nell'altra.
Inoltre, tutta la corrente che circola ha la tendenza a creare un campo magnetico. Questi campi magnetici possono irradiarsi per qualche metro[4]. Quindi, chi ne ha i mezzi, potrebbe ricostruire il contenuto di una schermata o di ciò che è stato

scritto su una tastiera, e potrebbe farlo da dietro un muro, in strada o dall'appartamento accanto. Con questo metodo, dei ricercatori sono riusciti a registrare da una distanza di 20 metri ciò che era stato digitato su una normale tastiera via cavo, partendo dalle emissioni elettromagnetiche che essa emanava[5].

4 Berke Durak, attraverso l'utilizzo di un semplice walkman capace di ricevere la radio, nel 1995 è riuscito a captare le onde elettromagnetiche emesse dalla maggior parte dei componenti del proprio computer [http://nbl.gs/qg].
5 Martin Vuagnoux e Sylvain Pasini hanno realizzato degli spaventosi video per illustrare il loro studio *Compromising Electromagnetic Emanations of Wired and Wireless Keyboards*, pubblicato nel 2009 [http://nbl.gs/qgu].

Lo stesso tipo di operazione è possibile partendo dall'osservazione dei leggeri disturbi che genera il computer all'interno della rete elettrica a cui è attaccato[6].
Altre esperienze, che consistono nell'ascoltare con un microfono il rumore dei componenti elettronici del computer o quello della sua alimentazione elettrica, hanno permesso in certe condizioni di decifrare le chiavi di cifratura contenute sul computer bersaglio[7]. In seguito a questo fatto sono state pubblicate delle correzioni ai software coinvolti, in modo da rendere più difficile questo tipo di attacco. Infine, alcune periferiche (la tastiera, il mouse, le casse audio...) funzionano senza fili. Per farlo, comunicano con il computer attraverso le onde radio captabili e eventualmente decodificabili impunemente da chiunque stia intorno.
Per riassumere brevemente, anche se un computer non è connesso a una rete, e indipendentemente dai software che ci girano sopra, resta comunque possibile per delle persone ben equipaggiate "ascoltare" ciò che ci transita dentro.

1.4 Software

Dopo la lista dei componenti fisici che costituiscono un computer, occorre soffermarsi sull'elemento meno palpabile: il software.
All'epoca dei primissimi computer, ogni volta che si voleva eseguire una diversa operazione, si doveva intervenire fisicamente per cambiare la disposizione dei cavi e dei componenti. Adesso le cose sono molto cambiate: le operazioni da compiere per eseguire i diversi compiti sono divenute dei dati come gli

---

6 Paul Kocher, Joshua Jaffe e Benjamin Jun hanno pubblicato nel 1998 un rapporto che spiegava le differenti tecniche di analisi del consumo elettrico.
7 Clément Bohic, 2013, *Crittografia: basterà ascoltare il processore per decifrare le chiavi* [http://nbl.gs/qgv].

altri. Questi dati, che vengono chiamati "programmi", sono a loro volta caricati, modificati e manipolati da altri programmi ancora.
Questi ultimi generalmente sono scritti per riuscire a fare una sola cosa, e farla bene, in modo da restare comprensibili agli esseri umani che li progettano.
È solo attraverso l'interazione di decine di migliaia di questi programmi, che si riesce a realizzare i compiti complessi per i quali vengono generalmente utilizzati i computer ai giorni nostri.
L'effetto prodotto dal nostro cliccare su un'icona è quindi il lancio di una catena di eventi, una somma impressionante di calcoli, che causano degli impulsi elettrici che alla fine vanno a modificare un oggetto fisico (come quando masterizziamo un DVD, o come nel caso di un monitor che cambia i propri LED per mostrare una nuova pagina, o di un hard-disk che attiva o disattiva dei micro-interruttori per creare la sequenza di numeri binari che costituirà un file).

1.4.1 Il sistema operativo

Lo scopo di un sistema operativo è prima di tutto quello di permettere ai programmi di condividere l'accesso ai componenti materiali del computer. Il suo ruolo è anche quello di far comunicare i vari programmi tra di loro.
Un sistema operativo viene generalmente fornito con un software, sufficiente almeno a consentire l'avvio di altri programmi.
La parte fondamentale di un sistema operativo è il suo nucleo (il "kernel"), che si occupa di coordinare l'utilizzo delle risorse fisiche da parte dei programmi.
Per ciascun componente fisico del computer che vogliamo utilizzare, il kernel attiva un programma che si chiama "driver".

Esistono dei driver per le periferiche di ingresso/input (come la tastiera e il mouse), per quelle d'uscita/output (il monitor, la stampante, ecc.) e per quelle di archiviazione (DVD, penne USB, ecc.).
Il kernel gestisce anche l'esecuzione dei programmi fornendogli delle porzioni di memoria e ripartendo i tempi di calcolo del processore tra i diversi programmi che si vogliono far lavorare.
Oltre al kernel, i sistemi operativi odierni come Windows, Mac OS X o GNU/Linux (con Debian, Ubuntu, Fedora, per esempio) includono anche molti strumenti e ambienti grafici che permettono di utilizzare il computer cliccando semplicemente su delle icone
Il sistema operativo è in genere installato sull'hard-disk. È possibile però utilizzare invece un sistema operativo installato su una penna USB o masterizzato su un DVD. In quest'ultimo caso si parla di sistema "Live" (visto che sul DVD non si potrà compiere nessuna modifica).

1.4.2 Le applicazioni

Vengono chiamate "applicazioni" quei programmi che permettono di fare davvero ciò che stiamo chiedendo a un computer. Come esempi possiamo citare Mozilla Firefox come web browser, LibreOffice per le faccende d'ufficio o VLC per la musica e i video.
Ciascun sistema operativo definisce un metodo ben preciso con il quale le applicazioni possono accedere all'hardware, ai dati, alla rete e alle altre risorse.
Le applicazioni che vogliamo utilizzare devono quindi essere pensate per girare sul sistema operativo del computer sul quale vogliamo farle andare.

1.4.3 Le librerie

Invece che riscrivere per ogni applicazione pezzi di programma incaricati di fare le stesse cose, i software li condividono tra loro in librerie.
Esistono librerie per la visualizzazione grafica (che assicurano una coerenza in quello che viene mostrato sullo schermo), per la lettura e la scrittura dei formati dei file, per interrogare certi servizi di rete, ecc.
Se non siamo programmatori, raramente abbiamo bisogno di toccare le librerie. Può tuttavia essere interessante conoscere la loro esistenza, anche solo perché un problema (ad esempio un errore di programmazione) in una libreria può ripercuotersi su tutti i programmi che la utilizzano.

1.5 La memorizzazione dei dati

Abbiamo visto come un hard-disk (o una penna USB) consentano di conservare alcuni dati nel lasso di tempo tra un'accensione e l'altra del computer.
Ma per poterli ritrovare, i dati devono essere disposti in un certo modo: uno scaffale dove si accumulano semplicemente i fogli non sarebbe una delle forme di archiviazione delle più efficaci...

1.5.1 Le partizioni

Come un armadio, in cui si possono mettere vari ripiani, così è possibile "scomporre" un hard-disk in più partizioni.
Ciascun ripiano può avere un'altezza o una classificazione diversa a seconda che ci si voglia mettere libri o classificatori, in ordine alfabetico o in ordine di lettura. Allo stesso modo,

in un hard-disk ciascuna partizione potrà essere di grandezza diversa e contenere un diverso modo di organizzare le cose: questo è ciò che viene chiamato "file system".

1.5.2 I file system

Un file system serve prima di tutto a ritrovare le informazioni all'interno della nostra immensa mole di dati, nella stessa maniera in cui l'indice di un libro di cucina permette di andare direttamente alla pagina giusta per leggere la ricetta per una cena.
Attenzione però: eliminare un file è come tirare una riga sopra uno degli argomenti dell'indice, quindi sfogliando tutte le pagine del libro si può ancora ritrovare la nostra ricetta, almeno finché la pagina non viene sovrascritta. Ma di questo parleremo meglio più avanti[8].
Si possono inventare migliaia di formati diversi per organizzare i dati, e di conseguenza esistono molti tipi diversi di file system. Quando si parla di formattazione ci si riferisce alla creazione di un file system su un supporto.
Dato che è il sistema operativo a fornire l'accesso ai dati, il file system è spesso legato strettamente a un particolare sistema operativo.

> Per citarne qualcuno: NTFS e FAT32 sono quelli in genere usati per i sistemi operativi Windows; gli *ext* (`ext3`, `ext4`) sono spesso utilizzati sotto GNU/Linux; gli HFS, HFS+ e HFSX sono usati da Mac OS X.

È però anche possibile leggere un sistema operativo "estraneo" al sistema che si sta utilizzando, tramite un software

8 Cap. 4.3

adeguato. Windows per esempio è capace di leggere una partizione ext3, se si installa un software appropriato.
Una delle conseguenze di questa cosa è che su un computer possono esistere degli spazi di archiviazione non riconosciuti dal sistema operativo, ai quali non si può dunque accedere facilmente.

1.5.3 I formati dei file

I dati che manipoliamo sono generalmente raggruppati sotto forma di file. Un file ha un contenuto e anche un nome, una posizione (la cartella in cui si trova), una dimensione e altri dettagli a seconda del tipo di file system utilizzato.
Ma all'interno di ciascun file, i dati sono a loro volta organizzati diversamente a seconda della loro natura e del software usato per modificarli. Per differenziarli si parla di formati dei file.
In genere si mette, alla fine del nome di un file, un codice che chiamiamo talvolta "estensione", che permette di indicare il formato del file. Si può scegliere un'estensione o un'altra, modificarla, ma questo è più che altro a titolo indicativo, e non significa che cambiandola si cambi anche il formato del file.
Facciamo qualche esempio di estensione: per la musica, si usano spesso i formati mp3 o ogg, per i documenti di testo di LibreOffice si usa "OpenDocumentText" (odt), per le immagini si può scegliere tra jpeg, png o altri.
Così come i software, anche i formati possono essere *aperti* o *proprietari*[9]. I formati aperti sono definiti pubblicamente per impedire, tra le altre cose, che il loro utilizzo sia ristretto a un solo programma.
Certi formati proprietari vengono analizzati con la lente d'in-

9 Cap. 4.1

grandimento per poter essere utilizzati da altri programmi, ma la loro comprensione resta spesso imperfetta. È il caso del vecchio formato di Microsoft Word (doc) o quello di Adobe Photoshop (psd). Normalmente, tutti i dati ai quali il processore deve accedere, e quindi tutti i programmi e i documenti aperti, dovrebbero trovarsi dentro alla memoria volatile.

1.5.4 La memoria virtuale (swap)

Ma per riuscire ad aprire un sacco di programmi e di documenti contemporaneamente, i sistemi operativi moderni hanno un trucco: quando è necessario scambiano dei pezzi di RAM con uno spazio all'interno dell'hard-disk dedicato a questo scopo. Si parla in questo caso di "memoria virtuale" o di "swap".
Il sistema operativo arrangia insomma le cose in modo che il processore abbia sempre nella memoria viva i dati ai quali vuole realmente accedere. La swap è anche esempio di spazio di archiviazione al quale in genere non si pensa, memorizzato sull'hard-disk sia sotto forma di un grosso file attiguo (sotto Microsoft Windows e talvolta anche sotto Linux) sia in una partizione a parte (con Linux).
Torneremo in seguito sui problemi che pongono queste richieste di formato e spazio in termini riservatezza dei dati.

2 | Tracce da tutte le parti

Il normale funzionamento di un computer lascia numerose tracce di tutte quelle operazioni che ci facciamo sopra. A volte, queste tracce sono informazioni necessarie al suo funzionamento, altre volte vengono raccolte per permettere ai software di essere "più pratici".

2.1 Nella RAM

Abbiamo visto come il primo luogo di archiviazione delle informazioni su un computer sia la RAM[1].
Quando il computer è sotto tensione elettrica, la RAM contiene tutte le informazioni di cui si ha bisogno. Conserva dunque necessariamente le numerose tracce: ciò che viene digitato sulla tastiera (comprese anche le password), le schede aperte, i diversi eventi che hanno ritmato la fase di avvio del computer. Prendendo in mano un computer acceso, non è molto difficile tirarne fuori l'insieme delle informazioni contenute dentro la RAM, salvandole per esempio in una penna USB o inviandole a un altro computer attraverso la rete. E impadronirsi di un computer può essere talmente semplice che può essere fatto anche collegandocisi attraverso un iPod mentre siamo girati di spalle[2]. Una volta recuperate, le numerose informazioni che contiene la RAM possono essere sfruttate ad esempio per conoscere ancora meglio le persone che usano quel computer.
Quando si spegne l'alimentazione questi dati diventano illeggibili. Ma ci vuole un po' di tempo, il che potrebbe bastare

---

1 Cap. 1.2.3

2 Di questo caso se ne parla qui: Maximillian Dornseif, 2004, *0wned by an iPod*, e Bruce Schneier, 2006, *Hacking Computers Over USB* [http://nbl.gs/qhH].

per una persona mal intenzionata a recuperarne il contenuto. Questa operazione è chiamata "cold boot attack": l'idea è quella di copiare il contenuto della RAM prima che abbia il tempo di cancellarsi, in modo da sfruttarlo in seguito. È anche tecnicamente possibile portare la memoria di un computer appena spento a una temperatura molto bassa – nel qual caso se ne riesce a conservare il contenuto per ore o persino giorni[3]. Questo attacco deve essere eseguito però subito dopo lo spegnimento. Inoltre, se utilizziamo alcuni software di grandi dimensioni (ad esempio ritoccando un'immagine enorme con Adobe Photoshop o GIMP) prima di spegnere il computer, è probabile che le tracce che erano state precedentemente lasciate nella RAM vengano scoperte. È importante sapere che esistono dei software appositamente progettati per sovrascrivere il contenuto della RAM con dati casuali.

2.2 Nella memoria virtuale (swap)

Il sistema operativo utilizza, in alcuni casi, una parte del disco rigido per aiutare la RAM. Ciò accade soprattutto se il computer è molto utilizzato, ad esempio quando si lavora su immagini di grandi dimensioni, ma anche in molti altri casi, in maniera imprevedibile.
La conseguenza più imbarazzante di questo sistema, seppur molto pratico, è che il computer scrive sul disco rigido le informazioni contenute nella RAM... Informazioni potenzialmente sensibili, quindi, *che rimarranno leggibili anche dopo aver spento il computer.*
Con un computer configurato in modo standard, è quindi illusorio credere che un documento letto da una penna USB,

---

3 Per approfondire: J. Alex Halderman et Al., 2008, *Least We Remember: Cold Boot Attacks on Encryption Keys* [http://nbl.gs/qhI].

aperta anche con un software portatile[4], non lasci mai tracce sul disco rigido.
Per impedire a chiunque di accedere a questi dati, è possibile utilizzare un sistema operativo configurato per cifrare la memoria virtuale. Ne parleremo prossimamente.

2.3 Standby e ibernazione

La maggior parte dei sistemi operativi consente di "mettere in pausa" un computer. Viene utilizzato principalmente con i computer portatili, ma è ugualmente valido anche per i computer fissi.

2.3.1 Standby

Lo standby spegne i componenti principali del computer mantenendo il computer acceso in modo da poterlo riaccendere rapidamente. Come minimo, la RAM continuerà ad essere alimentata per conservare tutti i dati su cui stavamo lavorando, tra cui password e chiavi di cifratura[5].
In breve, un computer in standby protegge l'accesso ai dati tanto quanto un computer acceso.

2.3.2 Ibernazione

L'ibernazione (o sospensione) consiste nel copiare e salvare l'intero contenuto della RAM sul disco rigido per poi spegnere completamente il computer. Al successivo avvio, il sistema operativo rileverà la sospensione, ricopierà il backup nella

4 Cap. 4.4
5 Cap. 5

RAM e inizierà a lavorare di nuovo partendo da lì. Nei sistemi GNU/Linux, la memoria viene solitamente copiata nella swap[6]. Su altri sistemi in un file di grandi dimensioni, spesso nascosto.
Dal momento che è il contenuto della RAM ad essere scritto sul disco rigido, questo significa che tutti i programmi e documenti aperti, le password, le chiavi di cifratura e altro, possono essere trovati da chiunque accederà al disco rigido. Questo, finché non ci si riscriverà sopra.
Tuttavia, nel caso di cifratura dell'hard-disk[7] questo rischio è limitato: per accedere al backup della RAM verrà chiesta una password.

2.4 I log

I sistemi operativi hanno una forte tendenza a scrivere nel loro "diario di bordo" una storia dettagliata di ciò che producono.
I log sono proprio questo: dati utili per il funzionamento del sistema operativo, che possono essere utilizzati per correggere problemi di configurazione o altri bug.
Tuttavia, la loro esistenza a volte può essere problematica. Gli scenari esistenti sono moltissimi, ma gli esempi che seguono dovrebbero essere sufficienti a dare un'idea del rischio:

- con GNU/Linux, ogni volta che viene acceso un computer, il sistema mantiene la data, l'ora e il nome dell'utente che accede;
- con GNU/Linux, sono di solito conservati la marca e il modello di ciascun supporto rimovibile (disco esterno, penna USB...) che è stato collegato;
- con Mac OS X, si conservano le date in cui si è stampato

6 Cap. 1.5.4
7 Cap. 5

e il numero di pagine;
- con Windows, il “registro di sistema” salva il nome del software, la data e l’ora di installazione o disinstallazione di un’applicazione.

2.5 Salvataggio automatico e altre attività pianificate

Oltre ai log, è possibile che altre tracce di file, anche cancellate, rimangano sul computer. Anche se i file e il loro contenuto sono stati rimossi, parte del sistema operativo o un altro programma potrebbero averne conservata una copia deliberatamente. Ecco alcuni esempi:

- utilizzando Windows, Microsoft Office può mantenere nel menu “documenti recenti” il riferimento al nome del file già cancellato e talvolta anche mantenere file temporanei con il contenuto del file in questione;
- con GNU/Linux, un file vecchio può contenere al suo interno il riferimento al nome di un file precedentemente cancellato. E LibreOffice può conservare tutte le tracce di un file cancellato allo stesso modo di Microsoft Office. In pratica, ci sono dozzine di programmi che funzionano in questo modo;
- quando si utilizza una stampante, il sistema operativo copia spesso il file in sospeso nella “coda di stampa”. Il contenuto di questo file, una volta completata la fase di stampa, non sarà scomparso dall’hard-disk;
- con Windows, quando si collega un’unità rimovibile (penna USB, hard-disk esterno, CD o DVD), il sistema inizia spesso esplorandone il contenuto per poi poter fornire un software adattato alla sua lettura: questa esplorazione automatica lascia in memoria l’elenco di tutti i file pre-

senti sul supporto utilizzato, anche se nessuno dei file è stato consultato.

È difficile trovare una soluzione adeguata a questo problema. Un file, anche se perfettamente cancellato, probabilmente continuerà a esistere sul computer per un po' di tempo anche in una forma diversa. Una ricerca sui dati grezzi del disco consentirebbe di vedere se esistono copie di questi dati o meno... a meno che non siano stati solo linkati o memorizzati in una forma diversa, compressi per esempio.
Solo la sovrascrittura dell'intero disco[8] e l'installazione di un nuovo sistema operativo possono garantire che le tracce di un file vengano eliminate. E da un'altra prospettiva, l'uso di un sistema Live in cui il team di sviluppo abbia prestato molta attenzione a questo problema, assicura che queste tracce non vengano lasciate altrove tranne che nella RAM. Torneremo prossimamente sull'argomento.

2.6 I metadati

Oltre alle informazioni contenute in un file, vi sono informazioni che lo accompagnano di cui possiamo non accorgerci a prima vista: data di creazione, nome del software, computer, ecc. Questi "dati riguardo ai dati" sono comunemente chiamati "metadati".
Una parte dei metadati viene salvata nel file system[9]: il nome del file, la data e l'ora di creazione e modifica e spesso molte altre cose. Queste tracce sono lasciate sul computer – e questo di per sé potrebbe già essere un problema – ma generalmente non vengono salvate nel file.
D'altra parte, molti formati di file memorizzano anche i me-

8 Cap. 18
9 Cap. 1.5.2

tadati *all'interno* del file stesso. Saranno quindi trasmessi durante un'eventuale copia su una penna USB o quando si invia una e-mail o nella pubblicazione online. Queste informazioni possono essere note a chiunque abbia accesso al file.
I metadati registrati dipendono dai formati e dai software utilizzati. La maggior parte dei file audio consente di registrare il titolo del brano ed eseguire la canzone. I programmi di scrittura o i pdf registreranno il nome dell'autore, la data e l'ora della creazione e talvolta persino la cronologia completa delle ultime modifiche e quindi, potenzialmente, le informazioni che si pensava fossero state eliminate[10].
Formati immagine come tiff o jpeg, file fotografici creati da una fotocamera digitale o da un telefono cellulare, contengono metadati "exif". Questi possono contenere la marca, il modello e il numero di serie del dispositivo utilizzato, ma anche la data, l'ora e talvolta le coordinate geografiche dello scatto, per non parlare di una versione in miniatura dell'immagine. Sono questi metadati che metteranno fine alla latitanza di John McAfee, fondatore ed ex capo della società di sicurezza informatica con lo stesso nome[11]. Tutte queste informazioni tendono a rimanere dopo aver utilizzato un software di foto ritocco. Il caso dell'anteprima in miniatura è particolarmente interessante: molte foto disponibili su internet contengono ancora l'intera foto da cui è stato fatto il ritaglio... e con le facce dietro sfocate[12].
Per la maggior parte dei formati di file aperti, tuttavia, esiste un software per esaminare ed eventualmente eliminare i metadati. Ne parleremo nei prossimi capitoli della guida.

---

10 Per approfondire: Deblock Fabrice, 2006, *Quando i documenti Word tradiscono la fiducia* [http://nbl.gs/qhJ].

11 Per approfondire: Big Browser, 2012, *Vizio di forma – la bufala che ha portato all'arresto di John McAfee* [http://nbl.gs/qhK].

12 Maximillian Dornseif et Steven J. Murdoch, 2004, *Hidden Data in Internet Published Documents* [http://nbl.gs/qhL].

3 | Software malevoli, intrusi e altri spioni

Oltre alle tracce che l'intero sistema operativo lascia mentre sta girando, sui nostri computer possono esserci anche svariati intrusi. A volte installati a nostra insaputa (e che permettono per esempio di deviare i log[1] altrove), a volte inclusi invece nel software che abbiamo installato.
Questi informatori possono far parte di tecniche di sorveglianza, dalla "lotta alla pirateria" dei software proprietari[2], alla schedatura mirata di un individuo, passando per la raccolta dati per fare spam o altre truffe.
La portata di questi dispositivi aumenta fortemente quando il computer è collegato a internet. La loro installazione in questo caso è enormemente più facile se non si fa niente per proteggersi, e il recupero dei dati collezionati può essere fatto a distanza.
Coloro che raccolgono queste informazioni però non sono pericolosi tutti alla stessa maniera: dipende dai casi, dalle motivazioni e dai mezzi.
Gli autori di violenze domestiche[3], i siti internet in cerca di consumatori, le multinazionali come Microsoft, l'ispettore Clouseau, o la National Security Agency… così come tante altre persone e strutture spesso in concorrenza tra loro e che non formano certo una totalità coerente.
Per introdursi nel nostro computer non hanno acceso agli stessi passe-partout e non sono tutti in grado di usare il piede di porco così bene: per esempio, lo spionaggio industriale è una delle cause più importanti della sorveglianza più o meno

---

1 Cap. 2.4

2 Cap. 4.1.2

3 Catherine Armitage, 2014, *Spyware's role in domestic violence* parla dell'utilizzo di malware e altri strumenti tecnologici da parte di autori di violenze domestiche [http://nbl.gs/qgw].

legale e malgrado le apparenze, non dobbiamo credere che Microsoft ceda tutti i propri trucchi alla polizia francese[4].

3.1 Contesto legale

In ogni caso, la polizia e i servizi di sicurezza francesi dispongono al momento dei mezzi per mettere in atto sorveglianza informatica molto completa in piena legalità, appoggiandosi ai diversi "informatori" che presentiamo qui di seguito[5].
La "Legge di rinforzo alla lotta contro il crimine organizzato, il terrorismo e il loro finanziamento, e per migliorare l'efficacia e la garanzia della procedura penale" del 2016 include delle disposizioni di legge per consentire di installare dei captatori[6] che registrino e comunichino ciò che appare sullo schermo o ciò che le diverse periferiche (tastiera, webcam, scanner, telefono...) trasmettono al computer. L'installazione di questi

4 Microsoft, in partnership con l'Interpol, ha costruito una suite di strumenti chiamata COFEE (*Computer Online Forensic Evidence Extractor*) messa a disposizione delle polizie di una quindicina di paesi. Korben, 2009, *Cofee – La clé sécurité de Microsoft vient d'apparaitre sur la toile* [http://nbl.gs/qgx].

5 La situazione italiana da questo punto di vista presenta analogie e differenze rispetto all'attualità francese qui raccontata. Il che meriterebbe un discorso ben più approfondito di quello che possiamo fare in poche righe. Per farvi un'idea di come siamo messi in Italia al momento riguardo malware e dintorni, potete ascoltare questa puntata de *Le dita nella presa*, andata in onda su Radio Onda Rossa: http://nbl.gs/qgy [NdT]

6 Usiamo qui il termine "captatore" come viene usato nell'ambito legale, istituzionale e giornalistico in Italia, spesso in modo generico e poco chiaro: per captatore si intende uno strumento informatico pensato per facilitare l'investigazione e l'accumulo di prove digitali nell'ambito di un'indagine. Potremmo semplificare chiamandolo "malware" o "virus", visto che tecnicamente non esiste una vera e propria differenza con questo tipo di oggetto. Ma certamente il termine "virus" è ammantato di un'aura malefica e teppista, mentre "captatore" ha un che di decisamente più rassicurante e burocratico. [NdT]

captatori viene autorizzata ad essere effettuata da remoto o penetrando nel domicilio della persona sorvegliata per piazzare i software necessari. Queste misure non si applicano soltanto ai reati rilevanti di “terrorismo”, (come ad esempio quello di “proliferazione di armi di distruzione di massa”), ma anche a certi reati commessi da più persone (i reati “associativi”). Si può andare dal concorso nella “circolazione e soggiorno irregolare di uno straniero in Francia” passando per la “distruzione, degradazione e deterioramento di un bene”, ma anche in caso di semplice richiesta da parte del Procuratore della Repubblica per “urgenza risultante da un rischio imminente di contaminazione delle prove o di grave attentato persone o beni”.
La legge sull’informazione in Francia del 2015 dà più o meno gli stessi poteri ai “servizi informativi specializzati” per la “ricerca, la raccolta, lo sviluppo e la messa a disposizione del Governo di informazioni relative a problemi geopolitici e strategici oltre che a minacce e a rischi suscettibili di minacciare la vita della Nazione”.

3.2 I software malevoli

I software malevoli (spesso chiamati “malware”) sono dei programmi sviluppati con l’intento di nuocere: raccolta di informazioni, possesso di informazioni illegali, inoltro di spam, ecc.
I virus, i worm, i trojan, gli spyware, i rootkit (software che consentono di prendere il controllo di un computer) e i keylogger[7] fanno parte di questa famiglia. Alcuni di questi programmi possono appartenere a più di queste categorie contemporaneamente.
Per riuscire a installarsi su un computer, alcuni software malevoli sfruttano delle vulnerabilità del sistema operativo o

7 Cap. 3.4

delle applicazioni. Si appoggiano su degli errori di progettazione o di programmazione per ribaltare il funzionamento dei programmi a proprio vantaggio. Purtroppo sono state trovate molte di queste “falle di sicurezza” in molti software, e nuove ne vengono costantemente trovate, sia da chi cerca di correggerle, sia da chi vuole sfruttarle.

Un altro metodo corrente è quello di invogliare le persone che utilizzano un computer a lanciare il software malevolo nascondendolo all’interno di un programma apparentemente inoffensivo. È così che un semplice link a un video postato su un social network legato alla rivoluzione siriana ha portato di fatto gli utenti a scaricarsi un virus contenente un keylogger[8]. In questo caso l’attaccante non è obbligato a trovare delle vulnerabilità gravi nei software odierni. È particolarmente difficile assicurarsi che dei computer condivisi da diverse persone oppure dei computer che si trovano in luoghi pubblici come una biblioteca o un internet-point, non siano stati compromessi: è sufficiente che una sola persona un po’ meno attenta si sia fatta fregare.

Inoltre, la maggior parte dei software malevoli “seri” non lascia tracce immediatamente visibili della propria presenza, e possono essere difficili da scoprire. Il caso senza dubbio più complicato è quello delle vulnerabilità non ancora note, chiamate “zero day”, e che i software di anti-virus non sono grado di riconoscere, perché non ancora inventariate. È proprio una di queste vulnerabilità zero day che l’azienda VUPEN ha venduto alla NSA nel 2012[9].

> Nel 2006, Joanna Rutkowska ha presentato nel corso della conferenza *Black Bar* il malware *Blue Pill*. Questa presen-

8 Eva Galperin et Al., 2014, *Quantum of Surveillance: Familiar Actors and Possible False Flags in Syrian Malware Campaigns* [http://nbl.gs/qh2].

9 Grégoire Fleurot, 2013, *Espionnage: Vupen, l’entreprise française qui bosse pour la NSA* [http://nbl.gs/qh3].

> tazione dimostrava che era possibile scrivere un rootkit che sfruttasse le tecnologie di virtualizzazione per ingannare il sistema operativo e rendere in questo modo veramente difficile identificare la presenza del malware, una volta scaricato.

Questi software possono rubare le password, leggere documenti salvati sul computer (anche i documenti cifrati[10], se sono stati decifrati sul momento), neutralizzare i dispositivi di anonimato su internet, catturare degli screenshot e nascondersi dagli altri programmi. Ma possono anche usare il microfono, la webcam o altre periferiche del computer. Esiste un vero e proprio mercato specializzato dove si possono comprare questo tipo di programmi, personalizzati per differenti obiettivi. Questi software permettono di effettuare numerose operazioni: ottenere numeri di conti bancari, password degli account Paypal, di inviare spam, di partecipare all'attacco di un server saturandolo di richieste, ecc. Ma sono anche molto efficaci per spiare organizzazioni o individui specifici.

> Per fare un esempio dagli Emirati Arabi, un attivista per i diritti umani Ahmed Mansour, è stato vittima di un attacco condotto sul proprio smartphone. Gli è stato inviato un sms che conteneva un link a un virus. Questo virus permetteva alla persona che lo controllava di utilizzare in ogni istante la videocamera, il microfono e di sorvegliare le attività del telefono della vittima. L'attacco è stato scoperto e neutralizzato grazie a Citizen Lab[11].

I servizi investigativi e la polizia francesi hanno il diritto di utilizzare questo tipo di software, il che vuol dire che quasi sicuramente ne dispongono. Una suite di software di spionag-

10 Cap. 5.1

11 Andréa Fradin, 2016, *"Pegasus", l'arme d'une firme israélienne fantôme qui fait trembler Apple* [http://nbl.gs/qh4].

gio, attribuita ai servizi, è stata trovata per esempio soprattutto in Iran[12].
Nessuno è in grado di sapere quanti computer sono al momento infettati da software malevoli, ma alcuni ritengono si tratti di una cifra che va dal 40 al 90% delle installazioni di Windows. Quindi è altamente probabile trovarne uno sul primo Windows che incroceremo. Fino ad oggi, usare un sistema operativo minoritario (come GNU/Linux) diminuisce significativamente i rischi di infezione poiché, essendo meno richiesti, lo sviluppo di malware specifici risulta meno vendibile.
Possiamo intanto suggerire dei metodi per limitare i rischi:

- non installare (o non utilizzare) software di provenienza sconosciuta: non dare fiducia al primo sito web che si incontra[13];
- prendere sul serio, ovvero considerare, gli avvisi dei sistemi operativi recenti che tentano di mettere in guardia l'utente quando utilizza un software poco sicuro, o quando dicono che è necessario un aggiornamento di sicurezza;
- infine, limitare le possibilità di installazione di nuovo software: riducendo l'uso dell'utente "amministratore" e delle varie persone che ne hanno accesso.

3.3 Hardware per lo spionaggio

Gli attaccanti che vogliono mettere le mani sui segreti contenuti all'interno dei nostri computer, come abbiamo visto,

12 Martin Untersinger, 2015, *Dino, le nouveau programmeespion développé par des francophones* [http://nbl.gs/qh5].
13 Questo consiglio vale anche per le persone che utilizzano GNU/Linux. Nel dicembre 2009, il sito *gnome.look.org* ha diffuso un malware presentato come uno screensaver. Il software era scaricabile sotto forma di pacchetto Debian in mezzo a mille altri screensaver e sfondi [http://nbl.gs/qh6].

possono utilizzare dei software malevoli[14], ma possono anche usare dell'hardware che non ha niente da invidiare al buon caro vecchio James Bond.

Esiste tutta una gamma di strumenti più o meno facilmente disponibili che permette l'intrusione o l'esfiltrazione di informazioni a praticamente tutti i livelli di un computer. In seguito alla pubblicazione da parte di Edward Snowden di documenti confidenziali della NSA, è stato pubblicato un vero e proprio catalogo di spionaggio informatico sul quotidiano tedesco *Der Spiegel*[15].

Senza poterli elencare in modo esaustivo, all'interno di questo catalogo scopriamo: falsi connettori USB che permettono di ritrasmettere sotto forma di onde radio quello che transita tramite loro; minuscole cimici, installate nei cavi che collegano il monitor o la tastiera al computer, in modo da poter intercettare a distanza ciò che scriviamo o vediamo; e poi una valanga di materiale da spionaggio installato sul computer, sull'hard-disk, sul BIOS, ecc.

Il quadro non è molto incoraggiante e una seria revisione del proprio computer comporterebbe lo smontarlo da cima a fondo, con poche possibilità di essere in grado poi di riuscire a farlo funzionare di nuovo.

Detto ciò, questi strumenti non sono a disposizione di ogni tipo di avversario. Inoltre non c'è niente che ci induca a pensare che l'uso di tali strumenti sia diventato abituale, vuoi per ragioni di costo, di installazione o altri motivi.

In ogni caso ci addentreremo lo stesso un po' sul caso dei keylogger, che rientrano sia nella categoria degli strumenti di spionaggio, che in quella dei software malevoli.

---

14 Cap. 3.2

15 Spiegel, 2013, *Interactive Graphic: The NSA's Spy Catalog* [http://nbl.gs/qh7].

3.4 I keylogger

I keylogger, che possono essere sia hardware che software, hanno lo scopo di salvare di nascosto tutto quello che viene digitato sulla tastiera di un computer per poi poterlo ritrasmettere all'agente o alla persona che li ha installati.
Una volta piazzati, la loro capacità di salvare, tasto dopo tasto, tutto quello che viene digitato sulla tastiera gli permette di aggirare ogni dispositivo di cifratura[16] e di accedere direttamente a password, passphrase e altri dati sensibili.
I keylogger hardware sono dei dispositivi collegati alla tastiera o al computer. Possono assomigliare a degli adattatori, a delle schede d'estensione all'interno del computer (PCI o miniPCI) o integrarsi dentro la tastiera (tanto per farsi un'idea, molti modelli sono in libera vendita a una somma che va dai 40 ai 100 dollari). Quindi, se non li si cerca specificatamente, sono difficili da scovare.
Nel caso di una tastiera wi-fi, per ricostruire quali tasti sono stati premuti non c'è neanche bisogno di un keylogger: si intercettano le onde radio emesse dalla tastiera per comunicare con il ricevitore e poi si rompe la chiave di cifratura utilizzata, che nella maggior parte dei casi è abbastanza debole. Da una distanza minore è anche possibile registrare e decodificare le onde elettromagnetiche emesse dalle tastiere via cavo, comprese quelle integrate nel portatile.
I keylogger software sono molto più diffusi, perché possono essere installati a distanza (tramite un sito internet, attraverso un software malevolo, o altro) e generalmente per il recupero dei dati raccolti non richiedono un accesso fisico alla macchina (l'invio si può fare per esempio periodicamente via e-mail). La maggior parte di questi software registrano anche il nome dell'applicazione che sta girando, la data e l'ora in cui

16 Cap. 5.1

è stata eseguita e i tasti che sono stati digitati durante il suo uso. Negli Stati Uniti, l'FBI utilizza da molti anni i keylogger software[17].
L'unico modo per individuare un keylogger hardware è quello di familiarizzare con questi dispositivi e di fare regolarmente una verifica visiva della propria macchina all'interno e all'esterno, anche se il catalogo della NSA pubblicato alla fine del 2013 ci fa rendere conto di quanto sia difficile essere in grado di accorgersi di un keylogger appena più grande di un'unghia. Nel caso dei keylogger software, le strade da battere sono le stesse degli altri software malevoli[18].

3.5 Problemi di stampa?

Sembrerebbe quasi di aver fatto il giro di tutte le sorprese che i nostri computer possono riservarci... ma invece ci si mettono anche le stampanti ad avere i loro piccoli segreti.

3.5.1 Un po' di steganografia

Prima cosa da sapere: molte stampanti di fascia alta firmano il proprio lavoro[19]. Questa firma steganografica, chiamata "watermarking", si basa su dettagli di stampa molto leggeri, spesso invisibili a occhio nudo, e vengono inseriti sui documenti. Permettono di identificare in modo certo la marca, il modello e talvolta il numero di serie della macchina che ha stampato.

---

17 Nel 2000, l'utilizzo di un keylogger ha permesso alla FBI di ottenere la passphrase usata da un tramite della mafia di Filadelfia per cifrare i propri documenti [http://nbl.gs/qh8].

18 Cap. 3.2

19 L'Electronic Frontier Foundation cerca di mantenere una lista dei costruttori e dei modelli.

Si capisce bene il motivo per cui questi dettagli stanno lì: per poter risalire alla macchina a partire dai documenti. Tant'è vero che la persona che aveva diffuso nel giugno 2017 dei documenti top secret della NSA sull'inquinamento delle elezioni negli Stati Uniti del 2016 da parte di hacker russi, è stata beccata. C'erano ancora i marchi della stampante usata per stampare i documenti riservati quando li hanno pubblicati sul giornale *The Intercept*[20].

Inoltre ci sono altre tracce lasciate sui documenti a causa dell'usura della macchina – e questo succede con tutte le stampanti. Con l'età le testine di stampa si spostano, appaiono leggeri errori, i pezzi si usurano e tutto questo va a formare una vera e propria firma della stampante. Proprio come la balistica permette di identificare un'arma a fuoco a partire da un proiettile, è possibile utilizzare questi difetti per identificare una stampante a partire dalle pagine che stampa.

Per proteggersi in parte da questa cosa, è interessante sapere che i dettagli di stampa non resistono a una fotocopia ripetuta: fotocopiare la pagina stampata e poi fotocopiare la fotocopia ottenuta, consente di far sparire questi marchi. Ma d'altra parte... ne lasceremo sicuramente altri, le fotocopiatrici presentano dei difetti e talvolta dei marchi steganografici, simili a quelli delle stampanti. Insomma è un cane che si morde la coda e il problema diventa più che altro scegliere quali tracce si vogliono lasciare...

3.5.2 La memoria, ancora...

Alcune stampanti sono sufficientemente “evolute” da assomigliare più a un vero e proprio computer piuttosto che a un timbro.

Queste possono porre problemi anche a un altro livello, visto

20 Robert Graham, 2017, *How The Intercept Outed Reality Winner* [http://nbl.gs/qhA].

che sono dotate di memoria viva[21]: questa memoria, proprio come quella di un PC, conserverà la traccia dei documenti che sono stati trattati per tutto il tempo in cui la macchina è attaccata alla corrente... o finché un altro documento non copre quella traccia.
La maggioranza delle stampanti laser dispongono di una memoria viva che può contenere una dozzina di pagine. I modelli più recenti o quelli che comprendono uno scanner integrato, possono invece contenere diverse migliaia di pagine di testo.
Ancora peggio: alcuni modelli, spesso utilizzati per le grosse tirature come quelle delle copisterie, hanno a volte degli hard-disk[22] interni ai quali l'utente non ha accesso e che conservano anch'essi delle tracce – e, in questo caso, anche dopo essere staccati dalla corrente.

---

21 Cap. 1.2.3
22 Cap. 1.2.4

4 | Qualche illusione di sicurezza

Bene. Abbiamo cominciato facendo un tour delle possibili tracce involontariamente lasciate nel nostro computer e la quantità di informazioni che dei malintenzionati avrebbero potuto sottrarci. Ora non resta che mettere da parte qualche preconcetto.

4.1 Software proprietari, open source e liberi

Abbiamo visto che un software potrebbe fare un sacco di cose che non vorremmo. Perciò è necessario fare il possibile per ridurre il problema. Da questo punto di vista, ai software liberi possiamo dare una maggiore fiducia rispetto al cosiddetto software proprietario: vedremo perché.

4.1.1 La metafora della torta

Per comprendere la differenza tra software libero e proprietario, usiamo la metafora della torta. Per fare una torta, hai bisogno di una ricetta: è una lista di istruzioni da seguire, ingredienti da utilizzare e un processo di trasformazione. Allo stesso modo, la ricetta di un software si chiama “codice sorgente”. È scritto in una lingua che è pensata per essere comprensibile dagli esseri umani. Questa ricetta viene quindi trasformata in un codice interpretabile dal processore, un po’ come la cottura di una torta ci dà l’opportunità di mangiarla.
Il software proprietario è disponibile e “pronto da mangiare” come una torta industriale, senza la sua ricetta. È quindi molto difficile garantire i suoi ingredienti: è fattibile, ma il processo è lungo e complicato. Inoltre, rileggere una serie di milioni

di aggiunte, di sottrazioni, di letture e di scritti in memoria per ricostruirne lo scopo e il funzionamento, non è proprio la prima cosa che si fa con un computer.
Il software libero, invece, offre la ricetta per chiunque voglia comprendere o modificare il funzionamento del programma. È quindi più facile sapere cosa viene inviato al nostro processore e, quindi, cosa accadrà ai nostri dati.

4.1.2 Software proprietari: una cieca fiducia

Un software proprietario è un po' come una scatola impenetrabile: possiamo constatare ciò che viene richiesto al software, ha una bella interfaccia grafica, ecc. Ma non possiamo davvero sapere in dettaglio come funziona. Non sappiamo se è costretto a fare ciò che gli viene chiesto di fare o se fa anche altre cose. Per scoprirlo dovremmo essere in grado di studiare il suo funzionamento, il che è difficile da fare senza codice sorgente... quindi dobbiamo fidarci *ciecamente*.
Windows e Mac OS X in primis sono enormi scatole, ermeticamente sigillate, su cui vengono installate altre scatole altrettanto ermetiche (da Microsoft Office agli anti-virus), che possono fare molte cose in più rispetto a quelle che gli chiediamo.
Come, per esempio, riunire le informazioni che questi software potrebbero averci sottratto, o permettere l'accesso all'interno del nostro computer a *backdoor*[1] fornite insieme al software in modo che chiunque abbia la chiave possa hackerare i nostri computer. Dato che non possiamo sapere come è stato scritto il sistema operativo, possiamo immaginarci di tutto.
Dunque, lasciare che la riservatezza e l'integrità dei nostri dati

1 Le backdoor sono delle "porte di servizio" che si possono trovare all'interno di un sistema informatico e che permettono di aggirare i sistemi di controllo e le procedure di sicurezza del sistema stesso

si basino su programmi che devono essere considerati affidabili a scatola chiusa, è la più pia illusione di sicurezza. E installando questi software che sostengono sulla loro confezione di garantirci la sicurezza, mentre il loro funzionamento non è per nulla trasparente, non può certo risolvere i nostri problemi.

4.1.3 Il vantaggio di avere la ricetta: i software liberi

La maggior fiducia che possiamo accordare ad un sistema *libero* come GNU/Linux è principalmente correlata al fatto che abbiamo la "ricetta". Teniamo presente che non c'è nulla di magico: il software libero non lancia alcun "incantesimo di protezione" sui nostri computer.
Tuttavia, GNU/Linux offre maggiori possibilità di rendere l'uso dei computer un po' più sicuro, in particolare consentendo di affinare le configurazioni di sistema. Questo troppo spesso implica il possedere una conoscenza specializzata, ma almeno lo rende possibile.
Il mondo che si aggira attorno al software libero non è molto compatibile con l'introduzione di backdoor: è un modo di produzione collettivo, piuttosto aperto e trasparente, al quale partecipano persone molto diverse; insomma non è facile lasciare dei "regalini" all'interno di questi software senza che nessuno se ne accorga.
Tuttavia, tocca fare attenzione anche ad alcuni software che si definiscono "open source". Essi consentono sì l'accesso alle proprie viscere, ma hanno anche delle modalità di sviluppo chiuse e opache. La modifica e la ridistribuzione di questi software è nella peggiore delle ipotesi proibita e, nella migliore, autorizzata ma resa nella pratica quasi impossibile. Solo il team originario può sviluppare il codice sorgente, quindi si può considerare che in pratica nessuno lo leggerà nel dettaglio e nessuno controllerà realmente il suo funzionamento.

Questo è il caso ad esempio di TrueCrypt, il cui sviluppo è stato interrotto a maggio 2014. Si trattava di un software di crittografia il cui codice sorgente è disponibile, ma il cui sviluppo è fermo e la licenza limita la modifica e la ridistribuzione. Secondo noi, per poter definire un software open source si dovrebbe giudicare anche come viene messo in commercio, e non basarsi solo su una promessa.
A meno che... la distinzione tra software libero e open source diventi sempre più sfocata: buona parte del software libero più importante viene scritto da impiegati dell'IBM o simili, e non andiamo ogni volta a guardare da vicino cosa scrivono.
Un altro esempio da mostrare sono le statistiche di coloro che sviluppano il kernel di Linux – che è libero – e le aziende per cui lavorano, attraverso il numero di righe di codice sorgente modificate nell'ultimo periodo di tempo:

Organizzazione	**Percentuale**
Intel	20,4 %
AMD	8,7 %
Samsung	6,6 %
Red Hat	4,8 %
(Sconosciuto)	4,0 %
Linaro	3,8 %
SUSE	3,6 %
IBM	3,0 %
(Consulente)	3,0 %
Solarflare Comm.	2,3 %
MediaTek	1,8 %
Covium	1,8 %

Quindi non è impossibile che chi ha scritto in un angolo un pezzo di software su cui la comunità fa affidamento abbia potuto far scivolare all'interno pezzi di codice dannoso. Questo è stato anche il caso dell'errore noto come "Heartbleed". Se usiamo solo software libero fornito da una distribuzione GNU/Linux non commerciale, è improbabile che ciò accada, ma c'è comunque una possibilità. Dobbiamo allora affidarci a chi si occupa della distribuzione perché studi il funzionamento dei programmi che vi sono integrati.
È comunque importante ricordare che questa fiducia può essere valida solo se non si installano cose a caso nel nostro sistema. Ad esempio, su Debian i pacchetti ufficiali della distribuzione sono *firmati*, il che rende possibile controllarne l'origine. Ma se si installano pacchetti o estensioni per Firefox trovati su internet senza controllarli, ci esponiamo a tutti i rischi di malware[2].
Per concludere e non farci più illusioni: *gratis o no, non esiste un software che possa da solo garantire la privacy e l'intimità dei nostri dati*; per fare questo, ci sono pratiche associate all'uso di *determinati software*. Software scelti perché diversi elementi ci permettono di dare loro un certo livello di fiducia.

4.2 La password di un account non ne protegge i dati

Tutti i sistemi operativi recenti (Windows, Mac OS X, GNU/Linux) offrono la possibilità di avere utenti diversi sullo stesso computer. È importante sapere che le password che a volte proteggono questi account non garantiscono affatto la riservatezza dei dati.
È certo pratico e conveniente avere un proprio spazio con le

---

2 Cap. 3.2

proprie impostazioni (segnalibri, sfondi…), ma una persona che volesse avere accesso a tutti i dati del computer non avrebbe grossi problemi ad ottenerlo: basta collegare l'hard-disk a un altro computer o leggerlo con un altro sistema operativo[3].
Inoltre, se l'utilizzo di utente e password può avere alcuni vantaggi – ad esempio, la possibilità di bloccare lo schermo quando ci si allontana per alcuni minuti – è necessario tenere presente che ciò non protegge realmente i dati.

4.3 La "cancellazione" dei dati

Ne abbiamo già parlato[4]: il contenuto di un file diventato inaccessibile o invisibile non si volatilizza; ora spiegheremo perché.

4.3.1 La cancellazione di un dato non ne elimina il contenuto…

…e può essere molto facile trovarlo. Infatti, quando "cancelliamo" un file – mettendolo nel Cestino e poi svuotandolo – stiamo solo dicendo al sistema operativo che il contenuto di questo file non ci interessa più. Il sistema sta quindi eliminando la sua voce nell'indice dei file esistenti in modo da poter riutilizzare lo spazio per aggiungerci altro in futuro.
Ma potrebbero volerci settimane, mesi o anni prima che questo spazio venga *effettivamente* utilizzato per i nuovi file, dunque prima che i vecchi dati scompaiano effettivamente. Nel frattempo, se guardiamo direttamente ciò che è scritto sull'hard-disk, troviamo il contenuto dei file. È un'operazione abbastanza semplice, automatizzata da molti software di recupero o ripristino dati come PhotoRec.

---

3 Cap. 1.4.1
4 Cap. 1.5.2

4.3.2 Una possibile soluzione: riscrivere più volte i dati

Una volta riscritto lo spazio sull'hard dirk, diventa difficile trovare ciò che c'era prima. Difficile, ma non impossibile: quando il computer riscrive 1 su 0, il risultato è invece 0,95 e quando riscrive 1 su 1, 1.051[5]. Un po' come quando riusciamo a leggere su un taccuino ciò che era stato scritto su una pagina strappata via grazie alle depressioni create sulla pagina vuota sottostante.
Diventa molto difficile invece, se non impossibile, recuperare i dati quando vengono sovrascritti più volte da altri dati casuali. Il modo migliore per rendere inaccessibile il contenuto di questi file "eliminati" consiste quindi nell'utilizzare un software che garantisce questo tipo di scrittura multipla (azione chiamata "wipe" in inglese).

4.3.3 Qualche limite della possibilità di riscrittura

Anche se è possibile sovrascrivere più volte i dati su un hard-disk per renderli inaccessibili, ciò non garantisce la loro completa scomparsa.

Dischi "intelligenti"
I dischi attuali riorganizzano il loro contenuto in modo "intelligente": parte del disco è riservata per sostituire spazi eventualmente difettosi. Queste operazioni di sostituzione sono difficili da rilevare e non possiamo mai veramente essere certi che la posizione che stiamo riscrivendo sia quella in cui il file era stato originariamente scritto.
Per le unità USB e SSD (Solid State Drive), è corretto dire che

5 Per approfondire: Peter Gutmann, 1996, *Secure Deletion of Data from Magnetic and SolidState Memory* [http://sugate.vado.li/].

nella maggior parte dei casi in realtà si riscrive in un posto diverso. La memoria flash, che viene utilizzata dalle unità flash USB e dalle SSD, smette di funzionare correttamente dopo un certo numero di scritture e contiene chip che riorganizzano automaticamente il contenuto per diffondere le informazioni in posizioni diverse.
Prendendo in considerazione questi meccanismi, diventa difficile garantire che i dati che si desidera distruggere scompaiano veramente nel nulla.
Malgrado ciò, esplorare un hard-disk per esaminarne l'interno richiede tempo e significative risorse materiali e umane... investimenti che non sono così immediati e alla portata di tutti. Per i chip di memoria flash di una penna USB o SSD, anche se non immediata, l'operazione è più semplice: servono solo un saldatore e un dispositivo per la lettura diretta dei chip di memoria, come ad esempio il PC-3000 Flash SSD Edition, venduto come strumento professionale per il recupero dei dati su dispositivi flash danneggiati, al costo di circa 1.500 dollari.

File system "intelligenti"
Un altro problema sono i file system[6] "intelligenti". I file system sviluppati negli ultimi anni, come NTFS o ext4, tengono traccia all'interno di un log[7] delle modifiche successive apportate ai file. Dopo un arresto improvviso del computer, consentono al sistema di riprendere semplicemente le ultime operazioni da eseguire, invece di dover riesaminare l'intero disco per correggere le incoerenze. Nel farlo, potrebbero di nuovo aggiungere tracce su quei file che uno voleva vedere scomparire.

> *Ext4*, il file system attualmente più usato su GNU/Linux, può funzionare con diverse modalità e dentro ai log inserisce solo i nomi dei file e altri metadati, non il loro contenuto.

6 Cap. 1.5.2
7 Cap. 2.4

Anche altre tecniche, meno comuni, possono dare problemi: i file system con scrittura ridondante e che continuano a scrivere anche in caso di errore, come i file system RAID; i file system che eseguono immagini istantanee del sistema (gli "snapshot"); i file system che si nascondono nelle cartelle temporanee, come i client NFS (file system di rete); i file system compressi, ecc.
Infine, non dobbiamo dimenticare che il file, anche se perfettamente cancellato, potrebbe aver comunque lasciato delle tracce altrove[8].

Ciò che non si sa
Riguardo ai CD-RW o ai DVD ± RW (riscrivibili), sembra che non sia stato condotto alcuno studio serio sull'efficacia della riscrittura. Le attuali raccomandazioni sono quindi di distruggere metodicamente i supporti di questo tipo che potrebbero aver contenuto dati che vogliamo far sparire[9].

4.3.4 Quando "cancelliamo"

Non eliminiamo i file mettendoli nel Cestino. Ad esempio, quando si utilizza l'opzione "Cancella la cronologia" del browser Firefox, non si fa altro che "cancellare" i file. I dati diventano inaccessibili per Firefox, ma sono ancora accessibili all'interno dell'hard-disk.
Vale la pena sottolineare che la riformattazione di un hard-disk non ne cancella appieno il contenuto. Come nel caso della cancellazione dei file, la riformattazione non fa altro che rendere disponibile lo spazio dove si trovavano i contenuti precedenti, ma i dati rimangono fisicamente presenti sul disco. Allo stesso modo in cui distruggere il catalogo di una biblioteca non

8 Cap. 2
9 NIST, 2014, *Guidelines for Media Sanitization* [http://vugaso.vado.li].

fa automaticamente sparire i libri negli scaffali… Quindi possiamo sempre trovare i file dopo la riformattazione, come se fossero stati semplicemente “cancellati”. PhotoRec offre anche questo tipo di funzionalità.

4.3.5 E per non lasciare alcuna traccia?

Sfortunatamente, non esiste un modo semplice per risolvere radicalmente il problema. La soluzione meno difficile per ora, è avviare il computer con un sistema Live, come Tails, configurato per utilizzare la sola RAM. In questo modo è possibile non scrivere nulla sull’hard-disk o sulla swap[10] e mantenere le informazioni solo nella RAM, quindi solo fino a quando il computer rimane acceso.

4.4 Software portatili: una falsa soluzione

Il cosiddetto “software portatile” è un software che non è installato su un determinato sistema operativo, ma che può essere avviato da una penna USB o da un hard-disk esterno – e quindi portato con noi per avercelo su qualsiasi computer.
È diventato facile scaricare queste applicazioni da internet. Pacchetti portatili come “Firefox+Tor” o “Thunderbird+Enigmail” sono disponibili online.
Tuttavia, a differenza dei sistemi Live, utilizzano il sistema operativo installato del computer in cui vengono fatti girare (la maggior parte delle volte sono destinati a Windows).
L’idea alla base è di avere sempre il software di cui abbiamo bisogno, a portata di mano e personalizzato per il nostro uso. Ma “trasportare il desktop ovunque” non è necessariamente il

10 Cap. 1.5.4

modo migliore per preservare la riservatezza dei dati.
Diciamolo subito: questi software non proteggono le persone che lo utilizzano più di quanto faccia un software non portatile. Peggio ancora, per ragioni di marketing inducono nell'utente false sicurezze, attraverso enormi sciocchezze. L'estratto della seguente frase proviene dalla home page del sito Framakey, una serie di software portatili realizzati da Framasoft, un sito francese di promozione di software libero: "L'uso del software avviene in modo sicuro e senza lasciare alcuna informazione personale sulle macchine in cui si utilizza Framakey". Questo, sfortunatamente, non è corretto.

4.4.1 Principali problemi

Queste soluzioni "chiavi in mano" pongono dunque alcuni problemi piuttosto fastidiosi.

Ci saranno tracce sull'hard-disk
Se il software è stato reso portatile in modo corretto, non dovrebbe lasciare deliberatamente tracce sul disco rigido del computer. Ma in realtà, il software non ha mai il controllo assoluto. Ciò dipende, per la maggior parte delle volte, dal sistema operativo utilizzato, che potrebbe aver avuto necessità di sfruttare la memoria virtuale sul disco rigido[11] oppure lasciare diverse tracce nei log[12] o nei "documenti recenti". Tutto ciò rimarrà quindi sull'hard-disk.

Non c'è motivo di fidarsi di un sistema sconosciuto
Come abbiamo visto, molti sistemi operativi non fanno assolutamente nulla di ciò che crediamo[13] e dunque, poiché il

11 Cap. 2.2
12 Cap. 2.4
13 Cap. 3

software portatile utilizza il sistema installato sul computer su cui viene lanciato, potremmo essere esposti a malware.

Non sappiamo chi li abbia compilati, né come
Le modifiche apportate al software per renderlo portatile sono raramente verificate, anche se, di solito, non sono fatte dagli autori del software stesso. Pertanto, possiamo sospettare che il software possa contenere vulnerabilità di sicurezza, volontarie o no.
Più avanti affronteremo il problema "dell'igiene" minima da tenere quando si sceglie un software da installare o scaricare.

5 | Un modo per proteggersi: la crittografia

La *crittografia* è la branca della matematica che si occupa specificatamente di proteggere i messaggi. Fino alla fine degli anni 90, l'utilizzo di tecniche crittografiche non era concesso al grande pubblico. In molti Paesi esso è divenuto legale, tra le altre cose, per permettere ai servizi commerciali su internet di farsi pagare senza che i clienti si facessero rubare il proprio numero di carta di credito.
La *crittoanalisi* è quella parte che consiste nel "rompere" le tecniche crittografiche, permettendo per esempio di recuperare un messaggio che era stato protetto.
Quando si vuole proteggere un messaggio, si distinguono tre aspetti:

- riservatezza: impedire gli sguardi indiscreti;
- autenticità: essere sicuri circa l'autore del messaggio;
- integrità: essere sicuri che il messaggio non abbia subito modifiche.

Si possono desiderare tutte e tre queste cose, oppure se ne può volere soltanto una. Una persona che scrive un messaggio *confidenziale* vorrebbe poter negare di esserne l'autore (e quindi non vorrebbe che il messaggio fosse *a*utenticato). Oppure è possibile che si voglia certificare la provenienza (autenticare) e l'*integrità* di una comunicazione ufficiale diffusa pubblicamente (quindi in modo tutt'altro che confidenziale).
In ciascuno di questi casi si parla di "messaggi", ma le tecniche crittografiche si applicano di fatto a qualsiasi numero, ovvero a qualsiasi dato, una volta digitalizzato.
È importante notare che la crittografia non cerca di nascondere i messaggi, ma di proteggerli. Per nascondere dei messaggi, bisogna invece ricorrere a delle tecniche steganografiche (come

quelle utilizzate dalle stampanti di cui abbiamo parlato in precedenza[1]), che non spiegheremo ora.

5.1 Proteggere i dati dagli sguardi indiscreti

Come sanno bene i bambini che usano delle parole in codice o i militari che si comunicano gli ordini, il metodo più serio affinché dei dati possano essere compresi soltanto dalle persone "all'interno del segreto", è quello della *cifratura*.
La cifratura di un file o di un supporto di archiviazione permette di renderlo illeggibile a tutti coloro che non hanno il codice d'accesso (spesso una passphrase). Sarà comunque possibile accedere al contenuto, ma i dati assomiglieranno a una serie di numeri a caso, e saranno quindi illeggibili.
Spesso si dice "criptare e decriptare" invece di "cifrare e decifrare", il che può risultare confondente; i termini in realtà sono sinonimi.

5.1.1 Come funziona?

Servono tre concetti fondamentali per capire come si fa a cifrare un messaggio[2].
Il primo concetto: la *confusione*. Si deve offuscare la relazione tra il messaggio originale e il messaggio cifrato. Un esempio molto semplice è il "Cifrario di Cesare":

testo in chiaro:	ASSALTO TRA UN'ORA
	↓↓↓↓↓↓↓ ↓↓↓ ↓↓ ↓↓↓
testo cifrato:	DVVDOZR ZUD AQ RUD

1 Cap. 3.5

2 Il passaggio qui di seguito è un adattamento molto parziale del fumetto di Jeff Moser sull'algoritmo AES [http://nbl.gs/qhB].

$$\text{A} + 3 \text{ lettere} = \text{D}$$

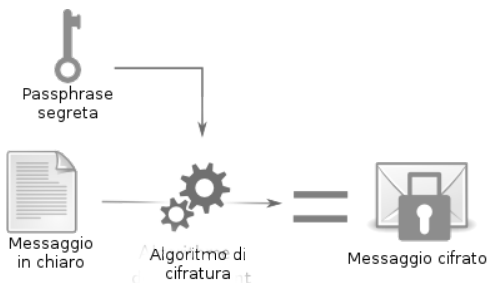
Però nel cifrario di Cesare è facile analizzare la frequenza delle lettere e risalire alle parole.
Quindi si passa al secondo grande concetto: la *diffusione*. Si sparpaglia il messaggio con lo scopo di renderlo più difficile da riconoscere.
Un esempio di questa tecnica è la trasposizione per colonne:

$$\begin{pmatrix}\text{A}\\\text{T}\\\text{U}\end{pmatrix} \begin{pmatrix}\text{S}\\\text{O}\\\text{N}\end{pmatrix} \begin{pmatrix}\text{S}\\\text{T}\\\text{O}\end{pmatrix} \begin{pmatrix}\text{A}\\\text{R}\\\text{R}\end{pmatrix} \begin{pmatrix}\text{L}\\\text{A}\\\text{A}\end{pmatrix} \xrightarrow[\text{diffusione in tre punti}]{} \begin{matrix}\text{ATU SON STO}\\\text{ARR LAA}\end{matrix}$$

Le diverse tecniche utilizzate per trasformare il testo originale sono ciò che viene chiamato "algoritmo di cifratura". Riguardo alla chiave di cifratura, si tratta, per esempio nel caso del cifrario di Cesare, del numero che indica di quanti caratteri si deve slittare (nel nostro esempio 3), oppure, nella tecnica della diffusione, del numero di linee delle colonne. Il valore di questa chiave è variabile, si può scegliere di fare delle colonne da due linee, o uno slittamento di sei caratteri.
Questo ci porta al terzo grande concetto: *il segreto risiede soltanto nella chiave*. Dopo qualche millennio, ci siamo accorti che non era una buona idea quella di partire dal presupposto che nessuno mai avrebbe capito l'algoritmo di cifratura. Prima o poi qualcuno finirà per scoprirlo... con la forza, se necessario.
Ai giorni nostri, l'algoritmo si può quindi trovare per intero su Wikipedia, dettagliato in lungo e in largo, in modo che chiunque possa verificare che non abbia particolari punti deboli. Questo perché l'unico modo per decifrare un testo sarà quello di disporre della chiave che è stata usata con quell'algoritmo.

5.1.2 Volete un disegnino?

Nel concreto, per assicurare la *riservatezza* dei nostri dati, si utilizzano due operazioni: cifrare e poi decifrare.

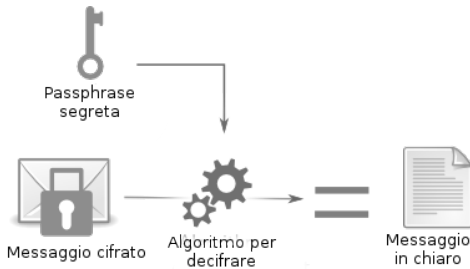
Primo passo: cifrare

Prendiamo il messaggio seguente per fare un esempio:

```
Gli spaghetti sono nella dispensa
```

Dopo aver cifrato questo messaggio utilizzando il programma GnuPG con l'algoritmo AES256, e come passphrase "questo è un segreto", si ottiene:


```
-----BEGIN PGP MESSAGE-----
jA0ECQMCRM0lmTSIONRg0lkBWGQI76cQOocEvdBhX6BM2AU-
6aYSPYymSqj8ihFXu
wV1GVraWuwEt4XnLc3F+OxT3EaXINMHdH9oydA92WDka-
qPEnjsWQs/oSCeZ3WXoB
9mf9y6jzqozEHw==
=T6eN
-----END PGP MESSAGE-----
```

Questo è quindi l'aspetto che assume un testo dopo la cifratura: il suo contenuto è diventato assolutamente incomprensibile. I dati in chiaro, leggibili, sono stati trasformati in un altro formato, illeggibile a chi non possiede la chiave.

Secondo passo: decifrare

Per decifrare, ci basterà utilizzare di nuovo GnuPG questa volta sul nostro testo cifrato. GnuPG ci chiederà la passphrase che prima ci era servita per cifrare, e se è giusta, ne otterremo l'informazione che ci mancava per preparare il pranzo.

5.1.3 Riguardo all'hard-disk

Se vogliamo tenere su un supporto di archiviazione (hard-disk, penna USB, ecc.) soltanto dati cifrati, sarà il sistema operativo che dovrà farsi carico "al volo" di effettuare le operazioni di cifratura e decifratura.
In questo modo, ogni volta che un dato viene letto dall'hard-disk, nel passaggio deve essere decifrato in modo che i programmi che ne hanno bisogno possano accedervi. Al contrario, ogni volta che un programma chiederà di scrivere un dato, questo verrà cifrato prima di essere salvato sull'hard-disk.

Affinché queste operazioni possano funzionare, è necessario che la chiave di cifratura si trovi nella memoria viva[1] per tutto il tempo che il supporto avrà bisogno di essere utilizzato.
Inoltre, la chiave di cifratura non può essere cambiata. Una volta che è stata usata per cifrare dei dati scritti sul disco, diventa indispensabile per poterli rileggere. Per cambiare la chiave, si devono quindi rileggere e poi riscrivere tutti i dati del disco.
Per evitare questa operazione faticosa, la maggior parte dei sistemi usati per cifrare i supporti di archiviazione si servono di un trucco: la chiave di cifratura in effetti è un grande numero, completamente casuale, che sarà a sua volta cifrato con l'aiuto di una passphrase[2]. Questa versione cifrata della chiave viene generalmente scritta sul supporto di archiviazione all'inizio del disco, in cima ai dati cifrati. Con questo sistema, cambiare il codice d'accesso diventa semplice, visto che basterà sostituire questa intestazione con una nuova.

5.1.4 Riassunto e limiti

La crittografia permette insomma di proteggere bene i propri dati, cifrando per intero o in parte l'hard-disk e gli altri supporti di archiviazione (penna USB, CD, ecc.) oppure cifrando le comunicazioni.
Inoltre i computer moderni sono abbastanza potenti da permetterci di rendere la cifratura un'operazione di routine, invece di riservarla a circostanze speciali o a delle informazioni particolarmente sensibili (che altrimenti verrebbero subito

1 Cap. 1.2.3
2 Il sistema LUKS, usato da GNU/Linux, permette anche di utilizzare diverse versioni cifrate della chiave di cifratura. Ciascuna di queste versioni potrà essere cifrata con una passphrase diversa, in modo da permettere a persone diverse di accedere agli stessi dati senza condividere lo stesso segreto.

identificate come importanti, e invece sarebbe meglio fossero confuse nella massa).
Si può anche predisporre una passphrase per cifrare l'intero hard-disk e/o dare accesso ad alcune persone a una parte cifrata con una loro passphrase. Si può anche cifrare singolarmente l'uno o l'altro file, o e-mail, o dividere in parti un file e cifrarle con passphrase differenti. Nonostante sia uno strumento potente ed essenziale per la sicurezza delle informazioni, la cifratura ha dei limiti – in particolare quando non è utilizzata correttamente.
Come spiegato prima, quando si accede a dei dati cifrati, bisogna avere ben chiare alcune cose. Prima di tutto, una volta che i dati vengono decifrati, essi risiederanno *come minimo* nella RAM. E poi, durante il tempo necessario a cifrare e decifrare, la RAM contiene anche la chiave di cifratura.
Chiunque disponga della chiave di cifratura potrà leggere *tutto ciò con la quale è stato cifrato*, e potrà anche servirsene per cifrare a sua volta dei dati.
Occorre quindi fare attenzione agli elementi qui di seguito:

- Il sistema operativo e i programmi hanno accesso ai dati e alla chiave di cifratura tanto quanto noi, per cui si tratta di stabilire quanta fiducia abbiamo in essi. Ancora una volta, si tratta di non installare cose a caso[3].
- Chiunque ottenga un accesso fisico al computer acceso ha, di fatto, accesso al contenuto della RAM[4]. Finché un disco cifrato è attivato, la RAM contiene in chiaro i dati sui quali ha lavorato dall'accensione del computer in poi (anche nel caso in cui questi dati siano cifrati sul disco). Ma soprattutto contiene, come abbiamo detto, la chiave di cifratura, che può quindi essere copiata. Perciò è meglio abituarsi, quando non lo si usa, a spegnere il computer e a

3 Cap. 3.2
4 Cap. 2.1

disattivare (smontare, espellere) i dischi cifrati.

- In certi casi, può essere necessario prevedere delle soluzioni materiali per staccare la corrente facilmente e rapidamente[5]; in questo modo i dischi cifrati torneranno inaccessibili senza la passphrase – a meno che non si effettui un cold boot attack[6].
- Anche in questo caso però potrebbe esserci un keylogger[7] sul computer, e questo registrerebbe la passphrase.
- Infine, può essere saggio ricordare che la matematica utilizzata negli algoritmi crittografici ha talvolta dei difetti. E molto più spesso ancora, i programmi che la applicano hanno delle fragilità. Alcuni di questi problemi possono trasformare, dall'oggi al domani, ciò che pensavamo la migliore delle protezioni in un semplice giochetto...

5.2 Verificare l'integrità dei dati

Abbiamo appena visto qualche metodo per assicurare la *riservatezza* dei nostri dati. Però a volte può essere anche importante essere sicuri della loro *integrità*, ovvero verificare che non abbiano subito modifiche (per sbaglio o di proposito). Possiamo anche volerci accertare della loro provenienza e verificarne l'*autenticità*.

In concreto, dopo la lettura di queste paginette, ci si può fare un'idea di quanto sia complesso essere sicuri che i programmi che installiamo sul nostro computer non siano stati modificati in corso d'opera per introdurre dei software malevoli[8].

---

5 Per questa ragione, è buona norma non lasciare la batteria attaccata a un portatile quando non viene utilizzato. In questo modo per spegnerlo basterà staccare il cavo.

6 Cap. 2

7 Cap. 3.4

8 Cap. 3.2

5.2.1 La potenza dell'ascia[9]

Le più importanti tecniche di verifica di integrità o di autenticità si fondano su degli strumenti matematici che la crittografia chiama "funzioni di hash".
Questi strumenti sono come delle grosse mannaie capaci di ridurre tutto in piccoli pezzi. Sappiamo che la nostra mannaia funziona abbastanza bene da poter essere utilizzata in crittografia se siamo in grado di dire che:

- avendo i piccoli pezzettini, è impossibile ricostruire l'oggetto originale senza provarli tutti;
- lo stesso oggetto, ogni volta che lo passiamo alla mannaia, darà sempre gli stessi piccoli pezzettini;
- due oggetti differenti devono dare due pezzetti differenti.

Se queste tre proprietà sono verificate, ci basterà allora confrontare i piccoli pezzi derivati da due oggetti per sapere se questi ultimi sono identici.
I piccoli pezzetti che vengono fuori dalla nostra mannaia si chiamano più comunemente "somma di controllo" o "impronta", e vengono in genere rappresentati sotto forma di qualcosa di simile a questo:

```
f9f5a68a721e3d10baca4d9751bb27f0ac35c7ba
```

Visto che la nostra mannaia funziona con dati di qualunque dimensione e forma, confrontare le impronte ci permette di confrontare più facilmente immagini, CD, software, ecc.
Però la nostra mannaia non è magica. Facciamo finta che in-

9 I francesi traducono gran parte dei termini tecnici inglesi. Così è anche per "hash", che in italiano lasciamo in inglese, e che in francese diventa invece "hache" (ascia) in riferimento al concetto del tagliare, estrapolare un pezzo dal codice [NdT].

vece a un certo punto riduca una cosa in piccoli cubetti di taglia identica: ci potremmo ritrovare con gli stessi cubetti usciti da due oggetti differenti. Questo si chiama "collisione". Questa carambola matematica è fortunatamente pericolosa solo quando è possibile provocarla... cosa già successa per molte funzioni di hash dopo qualche anno di ricerca, in particolare per la funzione SHA1[10].

5.2.2 Verificare l'integrità di un software

Facciamo un esempio: Alice ha scritto un programma e lo distribuisce in CD che si possono trovare tra le associazioni di utilizzatori di GNU/Linux. Betty vorrebbe utilizzare il programma di Alice, ma pensa che sarebbe molto facile per un amministratore malintenzionato rimpiazzare uno dei CD di Alice con un software malevolo.
Betty non può andare direttamente da Alice a prendere un CD, perché Alice abita in un'altra città. Però l'ha incontrata qualche tempo fa e sa riconoscere la sua voce. Quindi le telefona e Alice le detta la somma di controllo del contenuto del CD:

CD di Alice ⟶ `94d93910609f65475a189d178ca6a45f`
`22b50c95416affb1d8feb125dc3069d0`

Betty allora può confrontarla con quella generata a partire dal CD che si è procurata:

CD di Betty ⟶ `94d93910609f65475a189d178ca6a45f`
`22b50c95416affb1d8feb125dc3069d0`

10 Marc Stevens e Al., 2017, *Announcing the first SHA1 collision* [http://nbl.gs/qhG].

Siccome i numeri sono gli stessi, Betty è contenta e si sente sicura di stare utilizzando lo stesso CD che ha fatto Alice.
Calcolare queste somme di controllo non richiede molto più tempo che non la lettura completa del CD, giusto qualche minuto in più.
Invece adesso mettiamoci nei panni di Carole, che è stata pagata per prendere il controllo del computer di Betty a sua insaputa. Per fare questo ha creato un CD che sembra quello di Alice, ma che invece contiene un software malevolo.
Purtroppo per lei, l'hash funziona solo in un verso. Si deve quindi per prima cosa procurare il CD originale di Alice.
A quel punto, modifica questo CD introducendoci il software malevolo. Questa prima versione assomiglia molto all'originale e potrebbe ingannare più di una persona, ma lei sa che Betty verificherà la somma di controllo del CD.
Siccome Alice utilizza la funzione hash SHA256, che non ha difetti noti, a Carole non resta che provare un gran numero di varianti del suo CD, nella speranza di ottenere una collisione, ovvero la stessa somma di controllo di quella di Alice.
Sfortunatamente per lei, e fortunatamente per Betty, anche disponendo di molti computer potenti, le possibilità di riuscita di Carole in un tempo ragionevole (diciamo qualche anno) sono estremamente basse.
Per verificare l'integrità dei dati, basta insomma procurarsi un'impronta, o una somma di controllo, da degli intermediari di fiducia. Tutto sta poi a procurarsi queste impronte attraverso un mezzo di fiducia, ovvero di essere in grado di verificare la loro autenticità...

5.2.3 Verificare una password

Un altro esempio di utilizzo delle funzioni di hash riguarda la verifica dell'autenticità di una richiesta d'accesso.

Se l'accesso a un computer è protetto da password, come per esempio durante l'apertura di una sessione sotto GNU/Linux (ma ricordiamoci sempre che questa password non protegge i dati!), bisogna fare in modo che il computer possa verificare che la password che abbiamo messo sia quella giusta. Le password però non sono salvate in chiaro sul computer, sennò sarebbe troppo facile impadronirsene.
Allora come fa il computer a essere certo che la password immessa sia esatta?
Quando abbiamo scelto una password sul nostro computer, il sistema ha salvato, grazie a una funzione di hash, un'impronta della password. Per verificare l'accesso, lui "spezzetta" alla stessa maniera la password che abbiamo immesso. Se le impronte sono le stesse, decide che la password è giusta.
È insomma possibile verificare che le password corrispondano senza custodire la stessa password.

5.3 Simmetrica o asimmetrica?

Le tecniche di cifratura menzionate fin qui si basano su di una sola chiave segreta, che permette di effettuare sia la cifratura che la decifratura. In questo caso si parla di "crittografia simmetrica".
Questo per contrapporla alla "crittografia asimmetrica", che non utilizza la stessa chiave per entrambe le azioni. Anche detta "cifratura a chiave pubblica", quest'ultima viene usata soprattutto per la comunicazione online, di cui parleremo nel dettaglio in una prossima pubblicazione.
Una delle proprietà più interessanti della crittografia asimmetrica che può essere evocata brevemente è la possibilità di realizzare delle firme digitali. Come il suo equivalente sulla carta, una firma digitale permette di apporre un marchio di riconoscimento sui dati.

Queste firme digitali che utilizzano la crittografia asimmetrica costituiscono il modo più semplice per verificare la provenienza di un software.

SECONDA PARTE

Scegliere le risposte adatte

Ecco, adesso ci è preso il panico. Tutte le cose che facciamo ogni giorno con un computer ci tradiscono. Ancor più perché credevamo, a torto, di essere al sicuro. Oppure viene da chiederci, con una certa dose di scoraggiamento, se tutto sommato, abbiamo poi davvero qualcosa da nascondere... ma di questo abbiamo già parlato nella presentazione.
Tuttavia ci restano ancora dei margini prima di tornare ai vecchi metodi della botola nascosta sotto al tappeto in salotto, o alla porta segreta dietro la biblioteca che si apre azionando un falso libro (soluzioni dal sapore antico ma sempre ottime). Da qui in poi questo testo si occuperà di mappare questi margini. Nella parte che seguirà, mentre tratteremo alcuni concetti importanti perché d'interesse generale, svilupperemo anche in breve dei punti che mettano in grado chiunque di scegliere un insieme di pratiche e strumenti adeguati alla propria situazione. Successivamente descriveremo alcuni casi più comuni, che chiameremo "Esempi", per illustrare la nostra idea.

6 | Valutazione dei rischi

Quando ci si chiede quali misure adottare per proteggere i nostri dati o le comunicazioni digitali in generale, spesso si finisce per procedere un po' alla cieca. Primo perché la maggior parte delle soluzioni ha anche degli svantaggi: a volte sono soluzioni molto difficili da implementare, mantenere o utilizzare. Quando invece abbiamo possibilità di scelta, magari nessuna delle soluzioni risponde completamente alle nostre esigenze specifiche. Altre volte ancora sono soluzioni troppo nuove e non siamo sicuri che funzionino. E così via...
Per prima cosa dovremmo iniziare ponendoci alcune semplici domande per stabilire una "valutazione dei rischi"[1].

6.1 Cosa vogliamo proteggere?

Ciò che vogliamo proteggere rientra generalmente nella vasta categoria delle informazioni come, ad esempio, il contenuto di messaggi elettronici, i file di dati (foto, documenti, indirizzi e-mail) ma anche l'esistenza stessa di una corrispondenza tra due persone.
In questo contesto, la parola "proteggere" soddisfa diversi ambiti:

- la **riservatezza**: nascondere informazioni da occhi indesiderati;
- l'**integrità**: mantenere informazioni in buone condizioni e impedire che vengano in/volontariamente modificate;
- l'**accessibilità**: assicurarsi che le informazioni rimangano accessibili a chiunque ne abbia bisogno.

1 Per saperne di più: Electronic Frontier Foundation, 2015, *Une Introduction au Modèle de Menace* [http://zoreli.vado.li].

È quindi necessario definire, per ogni categoria di informazioni da proteggere, la necessità e il grado di riservatezza, di integrità e di accessibilità. Sapendo che queste esigenze spesso sono in conflitto tra di loro e che per questo sarà necessario d'ora in avanti definire le priorità e fare dei compromessi. In termini di sicurezza informatica, è difficile salvare capra e cavoli.

6.2 Da chi vogliamo proteggerci?

Ci viene in fretta la curiosità di capire quali capacità tecniche possieda chi potrebbe arrivare a ciò che vogliamo proteggere. E qui diventa difficile, perché non è facile sapere cosa può fare davvero e quali sono i mezzi e il budget a sua disposizione. Seguendo le notizie di attualità e ricavandone altre altrove, ci renderemo conto che la situazione varia molto a seconda di chi c'è in ballo. Tra polizia locale e *Agenzia per la Sicurezza Nazionale degli Stati Uniti* (NSA), c'è un'enorme differenza riguardo a possibilità di azione, mezzi e tecniche impiegate.
Ad esempio, la crittografia[2] è uno dei modi più adatti per impedire a chi, per questioni legali, può impadronirsi di un computer per accedere a tutti i dati che contiene. Tuttavia le leggi attualmente in vigore in Francia ci hanno regalato un colpo di scena: durante un'indagine si è obbligati a fornire la chiave crittografica per consentire agli investigatori di avere accesso ai dati, in caso contrario si va incontro a sanzioni economiche piuttosto pesanti. Questa legge consente agli investigatori con scarsi mezzi tecnologici di agire contro questo tipo di difesa, anche se finora non conosciamo ancora alcun caso in cui questa legge sia stata applicata. Per quanto riguarda invece le organizzazioni che hanno più risorse, come la NSA o la DGSE (*Direction Générale de la Sécurité Intérieure*), non

2 Cap. 5.1

sappiamo nulla circa le loro reali possibilità. Quali conoscenze hanno nel campo della crittografia? Sono in possesso di vulnerabilità non divulgate che gli consentono di leggere i dati? Ovviamente non possiamo essere certi di cosa siano in grado di fare questi enti, ma il loro campo di intervento è allo stesso tempo limitato e i casi in cui rischiamo di imbatterci in loro sono pochi.
Un altro importante fattore da prendere in considerazione: i costi. Maggiori sono le risorse messe in campo, più complesse sono le tecnologie utilizzate, maggiore è il loro costo; ciò significa che saranno utilizzate solo in casi specifici e altrettanto importanti a seconda del tipo di persone coinvolte. Ad esempio, ci sono poche possibilità di vedere un computer sottoposto a innumerevoli test con costose competenze informatiche per una questione che riguarda, ad esempio, il taccheggio.
Pertanto, prima ancora di cercare una soluzione, la domanda che ci dobbiamo porre è chi potrebbe essere interessato ad accedere alle nostre informazioni sensibili, e di conseguenza capire così se è necessario cercare soluzioni complicate o no.
Ottenere la protezione totale di un computer è comunque impossibile, e in questa storia, si tratta più che altro di mettere dei bastoni tra le ruote a quelli che potrebbero volere ciò che cerchiamo di proteggere. Più crediamo che abbiano mezzi complessi, più i bastoni dovranno essere numerosi e solidi.
Valutare i rischi quindi e, prima di tutto, domandarsi quali sono i dati che si desidera proteggere e chi sono le persone coinvolte. Da qui, possiamo farci un'idea di quali mezzi abbiano a disposizione (o almeno, per quanto possibile, cercare di scoprirlo) e, di conseguenza, possiamo infine definire una *policy di sicurezza* adeguata.

7 | Definire una policy di sicurezza

La forza di una catena si valuta basandosi sull'anello più debole. Non ha senso installare tre enormi serrature su una porta blindata, accanto a una fragile finestra semi distrutta. Allo stesso modo, la crittografia di una penna USB[1] non ha molto senso se i dati memorizzati al suo interno vengono utilizzati su un computer che manterrà diverse[2] tracce in chiaro sull'hard-disk.
Questo esempio ci può far riflettere su qualcosa: le soluzioni mirate non servono, a meno che non facciano parte di un insieme coerente di pratiche. E ancora, le informazioni che vogliamo proteggere sono spesso correlate a pratiche che esulano dagli strumenti digitali. Quindi per definire delle risposte appropriate, i rischi devono essere valutati globalmente[3].
A una data situazione corrispondono determinati problemi, rischi, conoscenze... e quindi differenti opportunità di azione. Non esiste una soluzione valida per tutti in grado di risolvere ogni problema con una bacchetta magica. L'unico modo fattibile è imparare abbastanza per essere in grado di immaginare e mettere in atto una policy di sicurezza adeguata alla propria situazione.

7.1 Una questione di compromessi

Possiamo sempre proteggere meglio i nostri dati e le comunicazioni digitali in generale; non c'è limite alle possibilità di attacchi e di sorveglianza o ai dispositivi che possono essere usati per proteggersi. Tuttavia, ogni protezione da utilizzare in

1 Cap. 5.1
2 Cap. 2
3 Cap. 6

aggiunta ad altre comporta sicuramente uno sforzo in termini di apprendimento, ma anche di tempo. Non c'è solo lo sforzo iniziale – l'installazione – ma anche una complessità generica nell'utilizzo, o nel tempo impiegato a digitare password o ad eseguire lunghe e ripetitive procedure. Si arriva a focalizzarsi più sulla tecnica in sé che sulle cose che si vorrebbero fare col computer.

Per ciascuna situazione, si tratta quindi di trovare un *compromesso* adeguato tra l'usabilità e il livello desiderato di protezione.

A volte però questo compromesso *non esiste*: potremmo anche concludere che gli sforzi necessari per proteggersi da un rischio plausibile sono troppo dolorosi, e che preferiamo correre il rischio... oppure, semplicemente, potremmo non utilizzare strumenti digitali per memorizzare alcuni dati o per parlare di determinate questioni. Esistono altri mezzi di provata efficacia sul lungo periodo: alcuni manoscritti sono sopravvissuti per secoli, sepolti in vasi conservati nelle caverne.

7.2 Come fare?

Si tratta di rispondere alla seguente domanda: quale insieme di pratiche e di strumenti mi proteggerebbe a sufficienza dai rischi precedentemente[4] valutati?

Per rispondere dobbiamo iniziare dalle nostre pratiche quotidiane e farci altre domande ancora:

1. Con una determinata policy di sicurezza, quale tipo di attacchi proverebbero i miei avversari?
2. Quali strumenti userebbero?
3. Questi mezzi sono alla loro portata?

---

4 Cap. 6

Se avete risposto "sì" alla terza domanda, prendetevi il tempo per studiare le soluzioni che vi serviranno per proteggervi, poi immaginate i cambiamenti causati da queste soluzioni pratiche e le policy di sicurezza che ne seguiranno. Se pensate che sia fattibile, mettetevi nei panni dell'avversario e ponetevi le medesime domande.
Ripetete questo processo di riflessione, ricerca e immaginazione finché non troverete un percorso praticabile, un compromesso sostenibile.
In caso di dubbi, chiedete a un amico affidabile e competente in materia di mettersi nei panni dell'avversario: sarà contento che abbiate già fatto da soli il grosso del lavoro e si sentirà incoraggiato ad aiutarvi con le cose che sono fuori dalla vostra portata.

7.3 Qualche regola

Prima di dare un'occhiata più da vicino agli esempi concreti e alle policy di sicurezza da adottare, ci sono alcuni principi chiave, alcune scelte di campo da attuare...

7.3.1 Complesso vs semplice

In materia di sicurezza informatica, una soluzione semplice deve essere sempre preferita a una soluzione complessa.
Prima di tutto, perché una soluzione complessa offre più "superficie di attacco", vale a dire più posti dove possono apparire problemi di sicurezza, che non mancheranno.
In secondo luogo, più complessa è una soluzione, maggiore è la conoscenza necessaria da mettere in campo per immaginarla, implementarla, mantenerla... ma anche per esaminarla, valutarne la pertinenza e i problemi. Come regola generale,

quanto più complessa è una soluzione, tanto meno sarà stata sottoposta agli sguardi affilati ed esterni necessari a stabilirne la validità.
Più semplicemente, una soluzione complessa che non tenga conto dello spazio mentale di chi la metterà in pratica è più probabile che incorra in problemi di sicurezza dovuti alle complesse interazioni o a casi particolari difficili da rilevare.
Ad esempio, piuttosto che passare ore a cercare di mettere in piedi sistemi che proteggano il computer dagli attacchi che arrivano dalla rete, è meglio semplicemente staccarlo dalla rete, o, in certi casi, togliere proprio la scheda di rete[5]...

7.3.2 Liste autorizzate, liste bloccate (whitelist, blacklist)

La reazione più comune, quando si diventa consapevoli di una minaccia, è cercare di proteggersi. Ad esempio, dopo aver scoperto che un tale software lascia tracce delle nostre attività in un determinato file, ripuliremo regolarmente quel file. Per scoprire poi magari che lo stesso software lasciava altre tracce in un'altra cartella, e così via.
Questo è il principio delle *blacklist*: un elenco delle cartelle in cui sappiamo che sono archiviati i file temporanei, i software che inviano report, ecc. Questo elenco verrà stilato a colpi di scoperte e spiacevoli sorprese, e in base ad esso cercheremo di fare del nostro meglio per proteggerci da ciascuna di queste minacce. Un elenco bloccato funziona insomma in base al principio "fiducia sempre, tranne che nei seguenti casi".
Il principio delle liste autorizzate (*whitelist*) funziona al contrario, perché è quello di "sfiducia sempre, ad eccezione dei seguenti casi". Blocchiamo *tutto*, *tranne* alcune eccezioni espli-

5 Cap. 1.2.5

citamente dichiarate. Non salviamo mai i file sull'hard-disk, tranne in quel posto o in quel momento preciso. Si vieta di accedere alla rete a tutti i software, tranne che ad alcuni specifici... Questi sono i principi di base.
Qualsiasi policy di sicurezza basata sul principio delle blacklist ha un grosso problema: l'elenco non sarà mai completo, perché prende in considerazione solo i problemi che sono già stati identificati. È un compito infinito, esasperante, quello di mantenere aggiornato un elenco bloccato; sia che lo facciamo noi stessi sia che lo deleghiamo a persone con competenze informatiche avanzate, in ogni caso ci sfuggirà sicuramente qualcosa.
Il problema è che nonostante i difetti, gli strumenti basati su un approccio di lista bloccata sono tantissimi (come vedremo), a differenza di quelli basati sul metodo di liste consentite, che quindi ci risulterà meno familiare.
Mettere in piedi un approccio whitelist richiede un grande sforzo iniziale che però può essere rapidamente ricompensato: imparare ad utilizzare un sistema Live che non lascia tracce sull'hard-disk è un'operazione che prende diverso tempo, ma una volta terminata, possiamo considerare concluse le lunghe sessioni di pulizia del disco rigido, che vanno ripetute continuamente e restano comunque inefficaci perché basate sul principio delle blacklist.
Un altro esempio sono gli antivirus che mirano a prevenire l'esecuzione di programmi dannosi. Operando in base al principio della lista bloccata, i loro database devono essere costantemente aggiornati, e arrivano sistematicamente in ritardo. Un approccio diverso al problema, su modello whitelist, è quello di impedire l'esecuzione di qualsiasi programma non precedentemente registrato o di limitarne le azioni. Questa tecnica, chiamata "Mandatory Access Control", si appoggia su delle liste che in questo caso sono però elenchi degli *autorizzati*, e una lista obsoleta causerà al massimo il malfunzionamento di un software invece che l'intrusione nel computer.

Inoltre, quando è possibile, è molto più interessante dotarsi di strumenti che si appoggino su liste autorizzate il più vaste possibile, in modo da poter fare tutto ciò che vogliamo con i computer con una certa tranquillità – e appoggiarsi invece, quando non esiste una whitelist adeguata, su delle blacklist solide, di provenienza certa, avendo bene in mente il problema intrinseco a questo metodo.

7.3.3 Non siamo dei robot

Alcune pratiche molto impegnative possono essere diabolicamente efficaci... finché non si commette un errore. Quindi, prima di farne qualcuno, è meglio prevedere piuttosto che pagare i cocci rotti.
Ad esempio, una penna USB pensata per essere usata solo su computer che utilizzano free software a cui facciamo particolarmente attenzione può comunque finire per essere dimenticata su un tavolo ed essere attaccata a Windows da qualcuno che l'ha confusa con un'altra. Ma se l'avessimo invece formattata da subito con un file system[6] incompatibile con Windows, avremmo limitato il rischio...
Insomma, non siamo robot. È meglio darsi reali garanzie piuttosto che pensare di dover stare sempre attenti e vigili: in questo modo saremo anche più calmi.

7.3.4 Data di scadenza

Una volta definita la policy di sicurezza, non dimenticate di rivederla di volta in volta! Il mondo della sicurezza informatica si sta evolvendo molto rapidamente e una soluzione oggi

6 Cap. 1.5.2

considerata abbastanza sicura, potrebbe facilmente essere attaccabile l'anno prossimo.
Non dimentichiamo anche di pensare che nelle nostre policy di sicurezza è importante monitorare la vita dei software da cui dipendiamo: i bug di sicurezza, gli aggiornamenti[7] a volte con buone o cattive sorprese... Tutto ciò richiede un po' di tempo che dovremmo prevedere sin dall'inizio del nostro viaggio.

7 Cap. 23

Esempi

Prendiamoci una pausa dalla teoria, illustriamo le nozioni che abbiamo imparato finora attraverso qualche esempio. A partire da alcune situazioni date indicheremo delle soluzioni che permettano di definire una policy di sicurezza adeguata. Buona parte delle soluzioni tecniche verranno spiegate poi successivamente attraverso le singole “ricette”.
Dato che ci stiamo ancora muovendo nel contesto “offline”, gli esempi che faremo saranno in qualche modo un po’ artificiali: partono tutti dal principio che i computer di cui parliamo non vengano mai connessi a nessuna rete, tantomeno a internet.

8 | Esempio 1 - Una nuova partenza, per non dover più pagare i cocci rotti

(ovvero come fare le pulizie su un computer dopo anni di pratiche spensierate)

8.1 Contesto

Prendiamo un computer usato da qualche anno senza precauzioni particolari. Questa macchina avrà senza dubbio uno o più dei seguenti problemi:

1. il suo hard-disk conserverà le tracce[1] indesiderate del proprio passato;
2. il sistema operativo sarà un software proprietario (per esempio Windows), e infarcito di software malevoli[2].

Inoltre, vi saranno archiviati dei file scomodi in modo assolutamente trasparente. Probabilmente questo computer sarà stato utilizzato per varie attività comuni, tra le quali alcune, diciamocelo, perfettamente legali, tipo:

- ascoltare musica e guardare film presi da internet;
- aiutare dei migranti a preparare i propri documenti per la prefettura;
- disegnare un bel biglietto d'auguri per la mamma;
- scrivere della falsa documentazione semplificando parecchio le pratiche amministrative (per esempio gonfiare le buste paga, quando non ne possiamo più di vederci negato l'affitto di una casa);

---

1 Cap. 2

2 Cap. 3

- tenere aggiornata la contabilità familiare;
- creare testi, musica o video "terroristi" – o più precisamente, secondo la definizione europea di terrorismo[3], che "minacciano di causare [...] distruzioni di massa [...] a un'infrastruttura [...] suscettibile [...] di produrre perdite economiche considerevoli", "con lo scopo di [...] costringere indebitamente i poteri pubblici [...] ad acconsentire o all'astenersi dall'acconsentire un qualunque atto". Per esempio, rientrerebbero in questo caso gli impiegati di una qualunque compagnia telefonica che, nel corso di una lotta, minacciassero di mettere fuori uso il sistema di fatturazione permettendo così agli utenti di telefonare gratuitamente.

8.2 Valutazione dei rischi

8.2.1 Cosa vogliamo proteggere?

Applichiamo al caso presente le categorie che abbiamo definito quando parlavamo di valutazione dei rischi[4]:

- riservatezza/confidenzialità: evitare che un occhio indiscreto cada troppo facilmente sulle informazioni contenute nel computer;
- integrità: evitare che queste informazioni siano modificate a nostra insaputa;
- accessibilità: fare in modo che le informazioni restino accessibili al momento del bisogno.

3 Unione Europea, 2017, *Direttiva (UE) 2017/541 del Parlamento europeo e del Consiglio del 15/03/2017 sulla lotta contro il terrorismo* [https://miroto.vado.li].

4 Cap. 6

In questo esempio, l'accessibilità e la confidenzialità sono prioritarie.

8.2.2 Da chi vogliamo difenderci?

Questa è una questione importante: a seconda della risposta che diamo, la policy adeguata può variare completamente.

Gesto generoso, conseguenze giudiziarie
Il computer potrebbe essere oggetto di una perquisizione. Per esempio: vostro figlio ha generosamente regalato un grammo di fumo a un amico che, dopo essersi fatto beccare, ha raccontato alla polizia dove l'ha preso. Di conseguenza vostro figlio viene penalmente considerato un trafficante di stupefacenti. Da qui la perquisizione.
In questo genere di situazioni, anche il vostro computer molto probabilmente verrà esaminato dalla polizia, mettendo così in pericolo l'obiettivo della confidenzialità. La gamma dei mezzi che verranno probabilmente impiegati va dall'ispettore Clouseau, che accenderà il computer e cliccherà dappertutto, al perito giudiziario che esaminerà da molto più vicino l'hard-disk. In compenso è improbabile che in questa situazione vengano utilizzati dei mezzi extra-legali, normalmente nelle mani dei Servizi e dei militari.

Furto
Il computer potrebbe essere rubato durante un furto. Al contrario della polizia, i ladri probabilmente non sapranno che farsene dei vostri piccoli segreti... e non vi denunceranno. Alla peggio potrebbero ricattarvi per recuperare i dati. E d'altra parte è improbabile che mettano in campo grandi mezzi per trovarli all'interno dell'hard-disk.

8.3 Definire una policy di sicurezza. Ovvero... Possibili attacchi e soluzioni praticabili

Adesso fatevi le domande di prima, mettendovi dalla parte dell'avversario[5].

8.3.1 Primo stadio: quando per vedere basta aprire gli occhi.

1. Tipo d'attacco più praticabile: montare l'hard-disk su un altro computer, esaminarne il contenuto e trovare tutti i vostri piccoli segreti.
2. Strumenti necessari: un altro computer, di cui l'ispettore Clouseau si servirà per trovare il più grande tra i vostri segreti; un perito giudiziario saprà invece anche ritrovare i file che voi credevate di aver cancellato; Nostradamus ne dedurrà la data di germinazione delle vostre semine.
3. Credibilità dell'attacco: alta.

Adesso adattiamo di conseguenza le vostre pratiche. Contro questo tipo di attacco cifrare l'hard-disk[6] è la risposta ovvia: installare e utilizzare un sistema cifrato[7] è ormai relativamente semplice.
I passi per arrivarci saranno dunque:

1. Lanciare un sistema Live per effettuare le operazioni che seguiranno in un contesto relativamente sicuro.
2. Salvaguardare temporaneamente, su un disco esterno o una penna USB cifrati, i file che devono sopravvivere alla grande pulizia.

5 Cap. 7
6 Cap. 5
7 Cap. 15

3. Espellere/smontare e staccare questo supporto di archiviazione esterno; cancellare "davvero" l'hard-disk *interno* del computer.
4. Installare un sistema operativo libero, precisando al programma di installazione di cifrare l'hard-disk, compresa la memoria virtuale (swap)[8]. Copiare sul nuovo sistema i dati precedentemente salvaguardati.
5. Fare il possibile per eliminare i file dal supporto esterno in maniera "sicura", in modo tale da poter poi...
6. Cancellare il contenuto dei file che si trovano sul supporto di backup temporaneo, che potrà eventualmente poi servire di nuovo.
7. In seguito, di tanto in tanto, fare in modo che i dati cancellati senza precauzioni particolari non siano recuperabili successivamente. Si dovrà anche assicurarsi di aggiornare il sistema regolarmente, per poter parare i "buchi di sicurezza" che potrebbero essere sfruttati dai software malevoli[9].

Per effettuare questi passi, nei prossimi capitoli vi forniremo le ricette giuste:

- cifrare un disco esterno o una penna USB: cap. 18;
- utilizzare un sistema Live: cap. 14;
- archiviare dei dati: cap. 19;
- cancellare "davvero": cap. 17;
- installare un sistema cifrato: cap. 15;
- mantenere aggiornato un sistema: cap. 23.

Se questa strada ci sembra praticabile, poniamoci di nuovo le stesse domande.

---

8 Cap. 1.5.4

9 Cap. 3.2

8.3.2 Secondo stadio: il cassetto del comodino non è cifrato

1. Tipo di attacco: una copia dei file che cerchiamo di proteggere potrebbe essere anche nella stanza accanto, nel secondo cassetto del comodino, scritta su carta o su una penna USB.
2. Strumenti necessari: perquisizione, furto, o altre visite impreviste.
3. Credibilità dell'attacco: alta, è esattamente da questo tipo di situazioni che cerchiamo di proteggerci in queste pagine.

Ancora una volta, dobbiamo renderci conto che una policy di sicurezza[10], per essere tale, deve essere pensata nell'insieme. Senza un minimo di coerenza nelle pratiche, non serve a niente incaponirsi a usare password lunghe come un giorno senza pane[11].
È quindi tempo di mettere in ordine le carte nel comodino e di ripulire tutte le penne USB, i CD e i DVD che contengono dati che ormai abbiamo deciso di cifrare:

- archiviare su un supporto cifrato i dati da conservare;
- per le penne USB e gli hard-disk esterni: cancellarne "davvero" il contenuto[12];
- per i CD e i DVD: distruggerli e sbarazzarsi dei residui;
- decidere cosa fare dei dati precedentemente salvati: copiarli sull'hard-disk appena cifrato o archiviarli[13].

10 Cap. 7

11 Espressione francese per indicare quanto il tempo passi lentamente senza cibo; in italiano si direbbe diversamente, ma l'espressione ci piaceva [NdT].

12 Cap. 17

13 Cap. 10

8.3.3 Terzo stadio: la legge come mezzo di coercizione

1. Tipo di attacco: la polizia ha il diritto di esigere che le venga dato accesso alle informazioni cifrate, come abbiamo spiegato nel capitolo dedicato alla crittografia[14].
2. Strumenti necessari: una sufficiente perseveranza nelle indagini per applicare questa legge.
3. Credibilità dell'attacco: di nuovo, basta che la polizia pensi di poter trovare degli elementi di prova sul computer, ed esserne talmente convinta da volersi spingere fin qua. Nell'esempio delle indagini che partivano dal grammo di fumo è poco probabile, ma non impossibile.

Se la polizia arriva a esigere l'accesso ai dati cifrati, in pratica ci si dovrà porre la seguente domanda: le informazioni contenute nel computer mi faranno correre più rischi rispetto a quelli derivanti da un rifiuto di consegnare la password?
Insomma dipende da come ce la sentiamo. Cedere, in questa situazione, non rimette in discussione l'importanza della cifratura dell'hard-disk: permette almeno di sapere cosa è stato rivelato, quando e a chi.
Detto ciò, può essere bene organizzarsi per vivere in modo meno critico una situazione come questa: il nuovo obiettivo potrebbe essere quello di avere un hard-disk sufficientemente "pulito" in modo che non sia una catastrofe dover cedere di fronte alla legge, o nel caso in cui il sistema crittografico venga compromesso.
Come primo passo, spesso è possibile fare un compromesso riguardo all'accessibilità, almeno per i file che riguardano progetti finiti a cui non si ha bisogno di accedere spesso. Ne parleremo più avanti, nell'esempio sull'archiviazione[15].
Successivamente, c'è tutta la questione della compartimen-

14 Cap. 5
15 Cap. 10

tazione; anche se è effettivamente possibile aumentare globalmente il livello di sicurezza dell'insieme delle attività praticate... questo potrebbe rivelarsi troppo faticoso. Conviene quindi definire meglio i singoli bisogni, in termini di confidenzialità, delle attività che svolgiamo. E, a partire da questo, tirare le fila e decidere quali sono più "sensibili" delle altre e quali hanno bisogno di un trattamento di favore.
Il prossimo esempio[16] studierà questi trattamenti di favore, ma abbiate pazienza, finiamo prima di parlare di questo caso.

8.3.4 Quarto stadio: in rete

Tutto quando detto finora vale per un computer disconnesso dalla rete. Nel momento in cui si connette, ci sono tutta una serie di altri attacchi immaginabili. Li studieremo in una prossima pubblicazione.
Oltre ai problemi che abbiamo visto fin qui, rimangono ancora molti altri attacchi che possono minare la policy di sicurezza che avevamo definito.

8.3.5 Tipo di attacco: una falla nel sistema di cifratura

Come spiegato precedentemente, ogni sistema di sicurezza può rischiare di venire compromesso. Se l'algoritmo di cifratura usato viene violato, questa notizia farà probabilmente il giro del mondo, tutti lo sapranno e sarà possibile reagire.
Ma se quello ad essere compromesso è il modo in cui viene impiegato dentro al kernel Linux[17] non lo leggerete sul giornale ed è molto probabile che soltanto gli specialisti di sicurezza informatica ne saranno al corrente.

---

16 Cap. 9
17 Cap. 1.4.1

A meno che non abbiate modo di conoscere uno di questi strani esseri, un modo di tenersi al corrente è quello di iscriversi alla mailing-list degli annunci di sicurezza di Debian[18]. Le e-mail ricevute da quel giro sono scritte in inglese, ma contengono l'indirizzo della pagina in cui si può trovarne la traduzione in altre lingue. La difficoltà è quella di riuscire poi a interpretarle...
Detto questo, anche se il sistema di cifratura fosse stato compromesso, bisogna comunque che anche gli avversari lo sappiano... l'ispettore Clouseau non ne saprà niente, ma magari un perito giudiziario sì.
Inoltre, entrando nel campo della fantascienza, ricordiamo che è difficile sapere in anticipo cosa hanno in mano, in materia, militari e agenzie governative come l'NSA.

8.3.6 Tipo di attacco: cold boot attack

1. Tipo di attacco: abbiamo descritto il cold boot attack nel capitolo dedicato alle tracce che lasciamo in giro[19].
2. Strumenti necessari: accedere fisicamente al computer quando è acceso o spento da poco, ad esempio durante una perquisizione.
3. Credibilità dell'attacco: per quanto ne sappiamo noi, questo attacco non è mai stato utilizzato dalle autorità, almeno in modo pubblico. La sua credibilità è quindi debole.

Può sembrare superfluo proteggersi contro questo attacco nella situazione che abbiamo descritto finora, ma è sempre meglio prendere da subito delle buone abitudini, piuttosto che avere brutte sorprese in futuro. Quali abitudini? Eccone qualcuna che rende un po' più difficile questo attacco:

18 https://lists.debian.org/debiansecurityannounce/
19 Cap. 2

- spegnere il computer quando non lo si usa;
- prevedere la possibilità di staccare la corrente facilmente e rapidamente: interruttori delle ciabatte accessibili facilmente, rimuovere la batteria del portatile quando è attaccato alla corrente (in modo che basti staccare il cavo per spegnerlo);
- rendere più lungo e difficile l'accesso all'alloggiamento che contiene la RAM, per esempio incollandolo o saldandolo.

8.3.7 Tipo di attacco: occhi e videosorveglianza

Con il sistema di cifratura che ci siamo immaginati nel primo passo, la riservatezza dei dati confida sul fatto che la password venga mantenuta segreta. Se viene digitata davanti a una videocamera di sorveglianza, un avversario che abbia accesso a questa videocamera o alle sue eventuali registrazioni potrà scoprirla e poi usarla sul computer per avere accesso ai dati. Ancora più semplicemente, uno sguardo attento, dentro un bar, potrebbe cogliere la vostra password mentre la digitate.
Mettere in atto questo attacco necessita di tenere sotto sorveglianza le persone che utilizzano quel computer, fino a quando una di loro digiterà la password nel posto sbagliato. Questa operazione può comportare diverso tempo ed è costosa.
Nell'esempio che stiamo studiando, un attacco così sarebbe pura fantascienza; attualmente sono poche le organizzazioni che possono mettere in campo mezzi così specifici, tranne che i diversi servizi speciali: anti-terrorismo, spionaggio industriale... Per premunirsi da un tale attacco, conviene:

- scegliere una password lunga[20], che rende molto complicato che un osservatore umano la memorizzi "al volo";

20 Cap. 12

- guardarsi intorno alla ricerca di eventuali occhi (umani o elettronici) indesiderabili prima di digitare la propria password;
- nascondere la propria tastiera con l'aiuto dello schermo, nel caso di un portatile, o con un telo[21] (mantello, asciugamano...).

8.3.8 Tipo d'attacco: la partizione non cifrata e il firmware

Come abbiamo già spiegato nel dettaglio[22], un sistema "cifrato" non lo è interamente: il piccolo software che all'avvio del computer ci chiede la password per decifrare il resto dei dati è, a sua volta, contenuto in chiaro sulla parte del disco che si chiama `/boot`. Un attaccante che ha accesso al computer può agevolmente, nel giro di qualche minuto, modificare questo software e installarci sopra un keylogger[23] in grado di salvarsi la password e poi farsela inviare in rete o venire a prendersela più tardi.
Se questo attacco viene progettato per tempo, l'avversario potrà in seguito decifrare l'hard-disk quando avrà di fronte il computer, durante una perquisizione, per esempio.
I mezzi impiegati in questo attacco sono, tutto sommato, abbastanza limitati: non occorre essere Superman per avere accesso qualche minuto alla stanza dove risiede il computer.
Ciò nonostante, nel caso descritto in questo esempio, si tratterebbe ancora di pura fantascienza. Talvolta però la realtà ha la tendenza a superare la finzione...

21 Nel film *Citizen Four* si vede Edward Snowden che si copre con una coperta mentre sta digitando la propria password.

22 Cap. 15

23 Cap. 3.4

Una protezione contro questo attacco è quella di tenere i programmi di avvio, tra cui questa piccola directory non cifrata (`/boot`), su un supporto esterno, ad esempio una penna USB, che verrà conservata in un luogo più sicuro del computer. In questo caso ciò che va protetto non è la *riservatezza* di questi dati, ma la loro *integrità*. Questa prassi esige un buon numero di competenze e di rigore.
Queste pratiche alzano il livello, ma c'è un però: una volta ottenuto l'accesso fisico al computer, se `/boot` non è accessibile né quindi modificabile, è comunque possibile effettuare lo stesso tipo di attacco sul firmware della macchina. È leggermente più difficile, perché come farlo dipende dal modello di computer usato, ma è fattibile. Non conosciamo in questo caso nessun modo praticabile di proteggersi.

8.3.9 Tipo d'attacco: i software malevoli

In precedenza[24] abbiamo capito che dei software installati a nostra insaputa su un computer possono rubare i nostri dati. In questo caso, un simile software è capace di trasmettere la chiave di cifratura dell'hard-disk a un avversario… che così otterrà, grazie a questa chiave, l'accesso ai dati cifrati, quando avrà poi accesso fisico al computer. Installare un software malevolo sul sistema Debian richiede delle competenze di più alto livello rispetto agli attacchi studiati finora, e anche più preparazione. Un attacco del genere, almeno nel caso della situazione di cui parliamo, è di nuovo fantascienza. In altre situazioni, bisognerà dare prova di una estrema prudenza riguardo alla provenienza dei dati e dei software che immettiamo nel computer, in particolare quando siamo connessi a internet… caso di cui, lo ricordiamo, non stiamo parlando in questa prima parte della guida.

24 Cap. 3.4

Quando abbiamo parlato dell'installazione dei software[25] abbiamo lanciato qualche consiglio utile sul come installare programmi in modo corretto. Più avanti, quando ci dedicheremo alla rete e a internet in particolare, entreremo meglio nel dettaglio.

8.3.10 Tipo d'attacco: il brute force

Attaccare un sistema crittografico con il "brute force", cioè cercare la password provando una per una tutte le combinazioni possibili, è il più semplice, il più stupido e il più lento dei metodi. Ma quando non si possono mettere in atto altri tipi di attacco...

Per decifrare in questo modo un hard-disk cifrato ci vuole moltissimo tempo (molti anni) e/o un'enormità di soldi e di competenze specifiche... se la password è solida.
Quello che possiamo dire è che, a priori, se un'organizzazione è disposta a investire tutte queste risorse per avere accesso ai

25 Cap. 16.2

vostri dati, preferirà di gran lunga mettere in atto uno degli altri attacchi elencati fin qui, meno costosi e altrettanto efficaci. Primo tra tutti quello di chiedere direttamente la password alla persona stessa, in modo più o meno cordiale...

9 | Esempio 2 - Lavorare su un documento sensibile

9.1 Contesto

Dopo la nuova partenza[1], il computer usato per portare avanti un progetto è stato dotato di un sistema cifrato[2]. Bene. Mettiamo il caso allora di dover lavorare a un progetto particolare, più "sensibile", per esempio:

- scrivere un volantino;
- disegnare un manifesto;
- impaginare un libro e poi esportarlo in pdf;
- organizzare una fuga di informazioni per divulgare le meschine pratiche di un datore di lavoro;
- montare un video e metterlo su un DVD.

In ciascuno di questi casi, i problemi da risolvere sono pressappoco gli stessi.
Siccome sarebbe troppo faticoso aumentare globalmente, di nuovo, il livello di sicurezza del computer, decidiamo che questo progetto in particolare deve beneficiare di un trattamento di favore.

9.1.1 Glossario

Nelle prossime pagine chiameremo:

- *documenti di lavoro*: l'insieme dei file necessari alla realizzazione del progetto (immagini o bozze, i documenti

1 Cap. 8
2 Cap. 15

salvati dal programma che utilizziamo, ecc.);
- *progetto*: il risultato finale (volantino, manifesto, ecc.).

9.2 Valutazione dei rischi

Partendo da questo contesto, cerchiamo adesso di definire i rischi ai quali veniamo esposti.

9.2.1 Cosa vogliamo proteggere?

Applichiamo al caso presente le categorie definite quando abbiamo parlato della valutazione dei rischi[3]:

- riservatezza: evitare che un occhio indiscreto arrivi troppo facilmente al progetto e/o ai documenti di lavoro;
- integrità: evitare che questi documenti vengano modificati a nostra insaputa;
- accessibilità: fare in modo che questi documenti restino accessibili quando ne abbiamo bisogno.

In questo caso accessibilità e riservatezza sono prioritarie. Accessibilità, perché l'obiettivo principale è quello di realizzare il progetto. Per quanto riguarda invece la riservatezza, dipende tutto da quanto il progetto vuole essere pubblico. Approfondiamo quindi la questione.

Opera a diffusione ristretta
Se il contenuto del progetto non è completamente pubblico, ovvero è segreto, si tratta di nascondere sia il progetto che i documenti di lavoro.

3 Cap. 6

Opera a diffusione pubblica
Se il progetto vuole essere pubblico, la questione della riservatezza si restringe a quella dell'anonimato.
Sono allora principalmente i documenti di lavoro che devono passare sotto silenzio: in effetti, trovarli all'interno di un computer potrebbe far dedurre che il suo proprietario abbia realizzato il progetto... con tutte le conseguenze spiacevoli che questo potrebbe comportare.
Ma non è tutto: se il progetto, o le sue versioni intermedie, sono salvate su questo computer (in un pdf, ecc.), la loro data di creazione è probabilmente registrata nel file system[4] e nei metadati[5]. Il fatto che questa data sia anteriore alla pubblicazione del progetto può portare degli avversari a trarre delle scomode conclusioni circa la sua generazione.

9.2.2 Da chi vogliamo difenderci?

Per farla semplice, riprendiamo le possibilità descritte nell'esempio che abbiamo fatto in precedenza sulla "nuova partenza"[6]: il computer utilizzato per realizzare il progetto potrebbe venire rubato, più o meno casualmente, sia dalle guardie che da dei ladri che lavorano per conto proprio.

9.3 Dipendenza da Windows?

Il primo problema che si pone è: quale sistema operativo usare? Dipende, evidentemente, dal software utilizzato per il progetto:

---

4 Cap. 1.5.2
5 Cap. 2.6
6 Cap. 8

- Se funziona sotto GNU/Linux, continuiamo nella lettura per studiare le varie possibilità che abbiamo.
- Se funziona esclusivamente sotto Windows, peccato. Vi proponiamo però lo stesso una via praticabile che permette di limitare i danni. Potete andare direttamente a leggere quella[7], saltando i capitoli che arrivano ora, dedicati invece a GNU/Linux.

9.4 Il sistema Live senza ricordi

I problemi riguardo a come iniziare, sono gli stessi del precedente esempio “una nuova partenza”[8]. Ma prima di mettere in campo le eventuali policy di sicurezza, lanciamoci in un rapido tour degli strumenti e dei metodi disponibili.

9.4.1 Liste bloccate vs liste autorizzate

Visto che abbiamo già un sistema Debian cifrato, potremmo in un primo momento immaginare di configurarlo in modo specifico per fargli conservare il minor numero possibile di tracce delle nostre attività sull’hard-disk. Il problema di questo approccio è lo stesso che vale per il metodo “lista bloccata”, e ne abbiamo spiegato i limiti nelle puntate precedenti[9]: per quanto tempo ci dedicheremo, qualunque esperto ci lavori, anche con una comprensione particolarmente approfondita dei meandri del sistema operativo usato, ci dimenticheremo sempre una piccola opzione nascosta bene, resteranno sempre delle tracce non volute alle quali non avevamo pensato.

---

7 Cap. 9.6
8 Cap. 8
9 Cap. 7.3.2

Al contrario, certi sistemi Live[10] funzionano in base al principio della lista autorizzata: a meno che non siamo noi a chiederlo esplicitamente, non viene lasciata nessuna traccia sull'hard-disk.
Occupandosi soltanto del criterio della "riservatezza", il metodo Live batte quindi l'altro 10 a 0. Il distacco viene un po' accorciato se consideriamo invece anche tempi e difficoltà di attuazione.

9.4.2 La botte piena o la moglie ubriaca?

Un sistema Live è effettivamente senza ricordi; questa proprietà è senza dubbio la sua principale risorsa, ma è anche fonte di inconvenienti. Per esempio, nel caso in cui la nostra Live preferita non fornisca un particolare software, che è tuttavia indispensabile per il progetto, dovremmo, a scelta:

- installare il software nella Live ogni volta che iniziamo una nuova sessione di lavoro;
- creare una penna USB avviabile Live che includa il nostro software all'interno di una partizione persistente;
- convincere gli autori della Live ad aggiungere quel software.

L'utilizzo di un sistema Live è la soluzione più sicura e, in questo caso, la meno difficile da attuare. Passiamo quindi a studiare una policy di sicurezza basata su questo sistema[11].
È anche possibile installare una Debian in una virtual machine[12], per rispondere a esigenze come questa, ma questa soluzione è abbastanza complessa e non ci sembra utile parlarne qui.

10 Cap. 14
11 Cap. 9.5
12 Cap. 22.1

9.5 Lavorare su un documento sensibile... dentro un sistema Live

Dopo aver spiegato il contesto all'inizio di questo esempio[13], e aver deciso di utilizzare un sistema Live, non ci resta altro che mettere in pratica questa soluzione... e studiarne i limiti.

9.5.1 Scaricare e installare il sistema Live

Non tutte le distribuzioni Live sono necessariamente pensate per delle pratiche "sensibili". Occorre quindi scegliere un sistema concepito in particolare per (provare a) non lasciare traccia sull'hard-disk del computer che stiamo usando.
Se non si dispone ancora di una copia dell'ultima versione di Tails, seguite la ricetta per scaricare e installare un sistema Live "discreto". (vedi ricetta relativa[14]).
A partire dalla prima periferica Tails appena creata, possiamo poi creare una penna USB dedicata solo al nostro progetto.
Per fare questo, bisogna far partire il sistema Live appena installato (vedi ricetta "avviare da supporto esterno", cap. 13).
Poi seguiamo le istruzioni per clonare una penna Tails (vedi ricetta "clonare un sistema Tails", cap. 14.3) e poi quelle per creare e configurare un volume persistente dentro Tails (vedi ricetta "creare la persistenza", cap. 14.5.1). Attiviamo soltanto l'opzione "Dati personali".

9.5.2 Installare un eventuale software aggiuntivo

Se abbiamo bisogno di utilizzare un software che non è incluso dentro Tails e che non vogliamo installare ogni volta, basta

13 Cap. 9.1
14 Cap. 14.2

seguire la ricetta per “installare un software aggiuntivo dentro Tails”[15].

9.5.3 Utilizzare il sistema Live

Ogni volta che dobbiamo lavorare sul nostro documento, basterà avere con noi la penna USB contenente la nostra Live e la sua persistenza cifrata per farcelo girare sopra. Per fare questo bisognerà attivare il volume della persistenza[16].

9.5.4 Distruggere il sistema Live

Una volta terminato il nostro progetto, stampato o pubblicato online, potremmo volerlo archiviare[17]. In seguito dovremmo distruggere il volume della persistenza[18].

9.5.5 Limiti

Alcuni limiti, comuni sia a questo metodo che a quello basato sull’uso di Windows, verranno esposti alla fine del capitolo.

9.6 Lavorare su un documento sensibile... sotto Windows

Dopo aver presentato il contesto all’inizio di questo esempio e una volta deciso, malgrado tutti i problemi che questo com-

---

15 Cap. 14.5.4
16 Cap. 14.5.2
17 Cap. 10
18 Cap. 14.5.3

porta, di utilizzare Windows, proviamo adesso a trovare un modo per limitare un po' i danni.

9.6.1 Cosa abbiamo: un colabrodo e una vecchia scatola di cerotti

Partiamo dal classico computer munito di un hard-disk con sopra Windows. Non vogliamo farla pesante, la prima parte di questa guida ha già abbondantemente descritto i molteplici problemi che questa situazione comporta. Un colabrodo insomma, pieno di buchi di sicurezza.
Proviamo ad appiccicare qualche cerotto su questo colabrodo. Eccone un rapido elenco.
Un hard-disk si può ogni volta smontare e nascondere. Certo. Ma ci sono i periodi in cui lo usiamo, a volte per molti giorni o settimane di fila. Questo cerotto è basato su due ipotesi un po' azzardate:

- *Dobbiamo avere fortuna.* Basta che il problema (una perquisizione, un furto...) si presenti al momento sbagliato per vanificare tutta la riservatezza desiderata;
- *La nostra autodisciplina deve essere perfettamente rigorosa.* Se ci dimentichiamo, o non abbiamo il tempo di "ripulire" l'hard-disk quando non ci serve più, e il problema si presenta proprio in quel momento, abbiamo perso: fine dei giochi.

Esistono degli strumenti per cifrare i dati su Windows. Possiamo fidarci o no, ma resta il fatto che essi si appoggiano per forza alle funzionalità di quella scatola nera che è Windows. Quini non possiamo far altro che diffidarne, e in ogni caso Windows avrà accesso ai nostri dati in chiaro e nessuno sa cosa potrebbe farci.

Per concludere questo piccolo giro nel cuore dei miracoli improbabili, aggiungiamo che la sola “soluzione” possibile nell’esempio in cui ci troviamo è usare un approccio a lista bloccata, di cui abbiamo già spiegato l’inefficacia[19].
Adesso passiamo alle cose serie.

9.6.2 Secondo passo: rinchiudere Windows in un compartimento (quasi) stagno

Quella che comincia ad assomigliare a una soluzione seria, è il far funzionare Windows all’interno un compartimento stagno, nel quale quando serve e con coscienza di causa, possiamo aprire una porta per permettergli di comunicare con l’esterno in un modo strettamente limitato.
In altri termini, mettere in piedi una soluzione basata su una logica del tipo lista autorizzata: a priori niente potrà entrare o uscire da Windows, e a partire da questa regola generale, autorizzeremo delle *eccezioni*, caso per caso, riflettendo sul loro impatto.
La *virtualizzazione* permette di mettere in atto questo tipo di sistema. È un insieme di tecniche materiali e logiche che permettono di far funzionare, su un solo computer, più sistemi operativi, in modo separato l’uno dall’altro, più o meno come se funzionassero su macchine diverse.
Ormai è anche relativamente facile far funzionare Windows *all’interno* di un sistema GNU/Linux, tagliandogli al tempo stesso tutti gli accessi alla rete e isolandolo da internet.

⚠ *Attenzione*: vi consigliamo di leggere questo capitolo *per intero* prima di precipitarvi sulle ricette pratiche; la descrizione dell’ipotesi seguente è abbastanza lunga, e i suoi limiti sono

19 Cap. 7

elencati alla fine di questo capitolo, dove suggeriamo anche delle contromisure. Sarebbe un po' un peccato passare quattro ore a seguire queste ricette, per poi rendersi conto che c'è un'altra soluzione, magari più adatta.

Cominciamo riassumendo l'ipotesi. L'idea è quella di far funzionare Windows all'interno di un compartimento stagno, *dentro* a un sistema Debian cifrato come quelli che abbiamo imparato a usare nell'esempio del capitolo precedente. Ciò che farà da hard-disk per Windows, sarà un grosso file salvato sull'hard-disk del nostro sistema Debian cifrato.

Installare il Gestore di macchine virtuali

La ricetta "installare il gestore di macchine virtuali"[20] spiega come installare il software di gestione per virtual machine, che ci servirà a lanciare Windows in un compartimento stagno.

Installare una versione "pulita" di Windows dentro il gestore di macchine virtuali

Prepariamo un'immagine del nostro disco virtuale: la ricetta "installare una versione di Windows virtualizzata"[21] spiega come installare Windows dentro a un gestore di macchine virtuali tagliandogli, *dall'inizio*, tutti gli accessi alla rete.
A partire da questo momento, Windows sarà un sistema *ospitato* da una versione cifrata di Debian.

Installare i software necessari al Windows "pulito"

Installare per prima cosa tutto il software *non compromettente*[22] che ci servirà a realizzare i nostri progetti: questo eviterà

20 Cap. 22.1
21 Cap. 22.2
22 Per esempio, se fosse necessario nascondere il fatto che abbiamo creato dei video, l'avere dei software di montaggio video potrebbe essere compromettente, e sarebbe più difficile da negare.

di doverlo rifare ogni volta quando si inizia un nuovo progetto… e eviterà, lo sottolineiamo bene, di utilizzare un'immagine di Windows "sporcata" per un nuovo progetto, una volta che magari siamo di fretta.
Visto che il Windows ospitato non ha il diritto di uscire dalla sua scatola per cercare da solo i file, occorre fargli arrivare "dall'esterno" i file di installazione dei software che ci servono.
Un'operazione come questa sarà anche utile, in seguito, per inviargli qualsiasi file, e riaverli indietro. Per il momento, visto che stiamo preparando un'immagine di Windows "pulita", che ci servirà come base per qualsiasi nuovo progetto, non mischiamo tutto e accontentiamoci di mandargli soltanto ciò che gli serve per l'installazione dei software non compromettenti che abbiamo scelto.
Sul sistema ospitante, creiamo una cartella chiamata Windows, e copiamoci *solo* i file necessari all'installazione dei software che vogliamo
Poi condividiamo questa cartella con il Windows ospitato: la ricetta "condividere una cartella con un sistema virtuale" spiega come procedere praticamente[23].
Per quanto riguarda l'installazione dei software all'interno di Windows: tutte le persone sufficientemente affezionate a Windows da leggere queste pagine, sono senza dubbio più competenti in materia di noi che stiamo scrivendo queste righe.

⚠ *Attenzione*: una volta effettuato questo passo, è imperativo *non fare nient'altro* all'interno di questo Windows virtualizzato.

Catturare un'istantanea del Windows "pulito"

Adesso facciamo un'*istantanea* della macchina virtuale che abbiamo appena preparato. Ovvero, salviamo il suo stato da

23 Cap. 22.6

una parte. In seguito questa istantanea ci servirà come base di partenza per ogni altro nuovo progetto.
La ricetta "Fare un'istantanea di una macchina virtuale"[24] spiega come effettuare questa operazione.

Nuovo progetto, nuova partenza
Mettiamo che un altro nuovo progetto necessiti dall'inizio dell'uso di Windows. Ecco come proseguire:

1. Ripristiniamo l'istantanea della macchina virtuale che contiene l'installazione del Windows "pulito";
2. Facciamo partire la macchina virtuale nel suo compartimento stagno; ci servirà *esclusivamente* per il nuovo progetto, e da quel momento diventerà una macchina virtuale "sporcata";
3. Dentro a questa nuova macchina virtuale sporca, viene creato un nuovo utente Windows; il nome deve essere diverso *per ogni nuovo progetto che sviluppiamo*, e questo utente deve servire *solo per fare questo*. Tutto ciò perché i software hanno la tendenza a scrivere il nome dell'utente attivo dentro i metadati[25] dei file che salvano, ed è meglio evitare certi recuperi inopportuni.

La ricetta "ripristinare lo stato di una macchina virtuale a partire da un'istantanea"[26] spiega i dettagli tecnici del primo punto. Per ciò che riguarda la creazione di un nuovo utente sulla versione di Windows che utilizziamo, crediamo di nuovo che chi ci legge sia in grado di trovare il modo di farlo attraverso il Pannello di controllo.
Ora che abbiamo un compartimento stagno, vediamo come aprire selettivamente delle porte, a seconda dei bisogni.

24 Cap. 22.3
25 Cap. 2.6
26 Cap. 22.4

Come inviare dei documenti a un Windows imprigionato?

Dato che il Windows ospitato non ha il diritto di uscire dalla propria scatola per andare a cercare da solo dei file, potrebbe essere necessario fargli arrivare "dall'esterno", per esempio:

- la materia prima (bozze, immagini o testi provenienti da altre fonti);
- un software necessario al nuovo progetto, e non presente nella immagine virtuale che abbiamo "scongelato".

Abbiamo già visto come procedere, ma qui ci troviamo in un caso molto particolare: l'installazione di nuovo software dentro il Windows pulito. Condividere dei file con un Windows sporcato richiede per prima cosa di riflettere e prendere precauzioni, cosa che andiamo adesso a studiare.
Il modo di farlo è leggermente diverso, a seconda del supporto sul quale si trovano in origine i file da importare (CD, DVD, penna USB, documento presente sull'hard-disk di un sistema cifrato), ma le precauzioni da usare sono le stesse:

- Windows deve avere accesso soltanto ai file che vogliamo importare, *solo a questo*. Non dobbiamo dargli accesso a una cartella che contiene alla rinfusa vari file che riguardano vari progetti che non devono invece essere collegati tra loro. Se questo comporta il dover prima smistare e riordinare, oh, sarà così;
- Se Windows ha bisogno di leggere (copiare) i file contenuti in una cartella, gli dobbiamo dare accesso *soltanto* a quella cartella. Meno permessi daremo a Windows di scrivere qua e là e meno tracce fastidiose lascerà in giro.

Per evitare di mischiare le cose, vi raccomandiamo di:

- creare *una* cartella di importazione per ciascun progetto;
- chiamare questa cartella nel modo più esplicito possibile, es. "cartella dove Windows può leggere";
- non condividere mai nessun'altra cartella con il Windows ospitato.

La ricetta "inviare file a un sistema virtualizzato"[27] spiega come procedere in pratica.

Come far uscire dei file da un Windows imprigionato? Il Windows ospitato di default non ha il permesso di lasciare tracce al di fuori del suo compartimento stagno. Ma è abbastanza inevitabile che arrivi il momento in cui sia necessario farne uscire dei file. Questi casi devono essere autorizzati esplicitamente, per esempio:

- per portare il file in copisteria, esportando un pdf;
- per proiettare, sotto forma di DVD, il film che abbiamo realizzato.

Per fare questa cosa, dobbiamo esportare i file dentro a una cartella vuota, dedicata a questo uso, e salvata dentro a un volume cifrato che può essere:

- una penna USB cifrata, che poi attiviamo sotto Debian scrivendo la password;
- l'hard-disk cifrato di Debian che ospita anche la macchina virtuale.

Questa cartella dedicata verrà condivisa con il Windows ospitato. Insistiamo sulle parole "vuota" e "dedicata": Windows potrà leggere e modificare tutto ciò che questa cartella contie-

27 Cap. 22.6

ne, e non sarebbe bello permettergli di leggere altri file quando c'è bisogno di esportarne solo uno. Se abbiamo bisogno di masterizzare un DVD, potremmo poi farlo girare su Debian. Per evitare di mischiare (di nuovo) le cose e per limitare il contagio, vi raccomandiamo di:

- creare una cartella di esportazione del progetto;
- chiamare questa cartella nel modo più esplicito possibile, es. "cartella dove Windows può scrivere";
- non condividere mai nessun'altra cartella con il Windows ospitato, tranne che l'altra cartella delle importazioni di cui abbiamo parlato prima.

Le ricette "condividere una cartella con un sistema virtuale"[28] e "cifrare una penna USB"[29] spiegano come procedere.

Quando il progetto è finito

Una volta terminato il progetto, bisogna fare le pulizie, ma prima di tutto:

1. esportiamo l'opera che ne è derivata su un supporto appropriato (carta, VHS, quel che sia…), aiutandoci con quello che abbiamo detto precedentemente per spiegare come far uscire dei file dal Windows ospitato;
2. i file di lavoro, se necessario, potrebbero dover essere archiviati (guarda caso il prossimo esempio parla proprio di questo[30]).

A questo punto viene il momento delle grandi pulizie, che elimineranno dal sistema ospitante la maggior parte possibile delle tracce lasciate dal progetto:

---

28 Cap. 22.6
29 Cap. 18
30 Cap. 10

- ripristiniamo l'immagine del disco al suo stato pulito con l'aiuto della ricetta "ripristinare lo stato di una macchina virtuale a partire da un'istantanea"[31];
- dopo aver verificato un'ultima volta che tutto ciò che deve essere conservato sia stato archiviato bene altrove, cancelliamo *davvero* i file condivisi con Windows[32];
- cancelliamo *davvero* le tracce lasciate sull'hard-disk[33].

9.6.3 Terzo passo: attacchi possibili e contromisure

L'ipotesi che abbiamo descritto finora si basa sull'utilizzo, come sistema ospitante, della Debian cifrata che abbiamo spiegato nel primo passo dell'esempio "una nuova partenza"[34]. Tutti gli attacchi che riguardano questa Debian sono quindi applicabili a questa soluzione.

Tracce lasciate sulla nostra Debian cifrata
La maggior parte delle tracce più *evidenti* di questo progetto sono separate dal resto del sistema: tutti i file di lavoro sono salvati dentro la cartella che contiene l'immagine del disco virtuale. Sul nostro sistema Debian vengono però lasciate delle tracce che riguardano il nome della macchina virtuale, la sua configurazione, i tempi di utilizzo.

a) Se la catastrofe arriva mentre stiamo realizzando il progetto: L'hard-disk del computer utilizzato contiene i file di lavoro contenuti nell'immagine del disco virtuale.

31 Cap. 22.4
32 Cap. 17.4
33 Cap. 17.7
34 Cap. 8.3

b) Se la catastrofe arriva dopo: L'immagine del disco virtuale dovrebbe essere stata ripulita nel momento in cui il progetto è finito, quindi se la catastrofe (cedere di fronte alla legge, la scoperta di un problema nel sistema crittografico...) arriva *dopo il fatto*, le tracce residue sull'hard-disk saranno meno evidenti e meno numerose che se avessimo proceduto normalmente.

c) Se la catastrofe arriva prima della fine del progetto, cioè prima della pulizia che abbiamo consigliato: Anche in questo caso sarebbe azzardato sentirsi protetti, perché come spiegato all'inizio di questo esempio[35] l'inconveniente peggiore del metodo descritto qui è quello dell'essere basato sul principio della lista bloccata, principio abbondantemente descritto in queste pagine[36]... e quindi resteranno sempre delle tracce indesiderate alle quali non avevamo pensato, oltre a quelle che ormai conosciamo bene[37]: log, memoria viva e memoria virtuale, salvataggi automatici.
Se nonostante queste preoccupazioni, l'ipotesi che vi stiamo descrivendo vi sembra un compromesso accettabile, tenete presente anche i limiti condivisi tra tutte le soluzioni studiate in questo esempio, limiti che descriveremo poco più avanti. Altrimenti, approfondiamo un po'.

Spingersi più lontano

Ammettiamo che uno degli attacchi descritti a partire dal terzo passo dell'esempio "una nuova partenza"[38] vi sembri credibile. Se esso riuscisse, il contenuto dell'hard-disk cifrato del sistema ospitante diventerebbe leggibile, in chiaro, dall'attaccante. Ora, i nostri file di lavoro sono, ricordiamolo, contenuti

35 Cap. 9.2
36 Cap. 7.3
37 Cap. 2
38 Cap. 8.3.3

dentro l'immagine del disco virtuale usato dal nostro Windows ospitato… il che non è nient'altro se non uno stupido file salvato sull'hard-disk del nostro sistema ospitante. Quindi questi file di lavoro, e tutte le tracce dei software usati dentro Windows, diventano leggibili dall'attaccante.
Prendiamo in considerazione dunque due strade che permettono di limitare i danni. Una è del tipo "lista bloccata", l'altra del tipo "lista autorizzata".

a) Non salvare l'immagine del disco virtuale dentro l'hard-disk del sistema ospitante: Un'idea è quella di salvare fuori dal disco del sistema ospitante l'immagine del disco virtuale usato dal sistema Windows ospitato. Per esempio, su un disco esterno cifrato. In questo modo, anche se il disco ospitante viene decifrato, i nostri file di lavoro restano inaccessibili… sempre che il disco esterno che li contiene sia in quel momento tenuto "ordinato".
Questo approccio è del tipo lista bloccata, con tutte le problematiche relative[39]. I file di lavoro e il sistema Windows si trovano sì da un'altra parte rispetto all'hard-disk del sistema ospitante, ma non dobbiamo dimenticare che questi dati saranno comunque utilizzati da un software che gira nel sistema ospitante stesso. In particolare, il gestore delle macchine virtuali. Come abbiamo spiegato nel capitolo "tracce da tutte le parti"[40], rimangono lo stesso diverse tracce, inevitabilmente.
Per seguire questa strada:

- informarsi sui limiti comuni[41] a tutte le soluzioni studiate in questo esempio;
- rifarsi alla ricetta per cifrare un hard-disk esterno[42].

39 Cap. 7.3.2
40 Cap. 2
41 Cap. 9.8
42 Cap. 18

b) Utilizzare un sistema Live come sistema ospitante: L'appendice di questo approccio a lista bloccata è una soluzione di tipo lista autorizzata, che coniuga l'utilizzo di un sistema Live con il salvataggio dell'immagine del disco virtuale su un hard-disk esterno cifrato. Per seguire questa strada:

- informarsi sui limiti comuni[43] a tutte le soluzioni studiate in questo esempio;
- rifarsi alla ricetta per cifrare un hard-disk esterno, e a quella che spiega come utilizzare un sistema Live[44].

9.7 Ripulire i metadati di un documento finito

Una volta che il nostro documento è finito, esportiamolo in un formato adatto allo scambio di documenti (per esempio pdf nel caso in cui dobbiamo stampare un testo, avi o ogv se si tratta di un video da caricare su internet, ecc.).
Mettiamo che stiamo pubblicando il nostro documento senza prendere altre precauzioni più ampie: un avversario in questo caso può prima di tutto molto semplicemente scaricare il documento e cercare eventuali metadati che lo possano condurre al suo autore. Malgrado le precauzioni che abbiamo già preso, sarà bene ripulire gli eventuali metadati presenti (vedi ricetta: "ripulire i metadati"[45]).

9.8 Limiti comuni a queste policy di sicurezza

Tutte le policy di sicurezza che abbiamo studiato in questo esempio sono vulnerabili a un certo numero di attacchi. Sia

43 Cap. 9.8
44 Cap. 18 e 14
45 Cap. 24

quelle basate su un sistema Live, che quelle che prevedono di incatenare l'infame Windows.
I passi 4 e 5 dell'esempio "una nuova partenza"[46], studiano alcuni attacchi che ci sono venuti in mente, più o meno fantascientifici, a seconda del momento storico, del luogo, dei protagonisti e delle circostanze in ballo. È il momento di ridargli una lettura.
Inoltre, la parte "problematica" di questa parte della guida è indirizzata, in un modo relativamente generico, ai molti metodi di sorveglianza che può essere bene ristudiare alla luce della situazione concreta di cui ci occupiamo. Facciamo attenzione in particolare alle questioni su elettricità, campi magnetici e onde radio[47], nonché agli effetti dei vari spioni[48].

46 Cap. 8
47 Cap. 1.3
48 Cap. 1.4.1

10 | Esempio 3 - Archiviare un progetto ultimato

10.1 Contesto

Siamo arrivati in fondo a un progetto sensibile[1], per esempio un libro è stato impaginato e stampato, un video è stato montato, compresso e caricato su un DVD.
In generale, da adesso non sarà più necessario poter accedere ai file di lavoro (immagini in alta risoluzione, bozze non compresse, elementi non inseriti…). Però potrebbe essere utile poterli ritrovare in seguito, per esempio per una riedizione, o un aggiornamento.
Visto che un sistema è tanto più suscettibile di essere *attaccato* quanto più lo si utilizza frequentemente, si possono togliere via dal computer che usiamo tutti i giorni le informazioni utilizzate raramente.
Inoltre è più facile riuscire a negare ogni legame con dei file se questi sono salvati su una penna USB seppellita in mezzo a un bosco, piuttosto che se vengono trovati archiviati sull'hard-disk del nostro computer di casa.

10.2 È così necessario?

La prima domanda da porsi prima di archiviare questo tipo di file è la seguente: è *davvero necessario* conservarli? Quando non si dispone più *del tutto* di una informazione, possono anche insistere, ma nessuno sarà in grado di darla, e questa a volte è la migliore soluzione.

1 Cap. 9

10.3 Valutazione dei rischi

10.3.1 Cosa vogliamo proteggere?

Cosa ci dicono le categorie definite quando abbiamo parlato di valutazione del rischio[2], applicate a questo caso?

- riservatezza: evitare che un occhio indiscreto arrivi troppo facilmente al progetto e/o ai documenti di lavoro;
- integrità: evitare che questi documenti vengano modificati a nostra insaputa;
- accessibilità: fare in modo che questi documenti restino accessibili quando ne abbiamo bisogno.

Qui, l'accessibilità è secondaria rispetto alla riservatezza: l'idea che sta alla base dell'archiviazione è quella di scendere a un compromesso, rendendo l'accesso ai dati più difficile *per tutti,* per offrire una maggiore riservatezza.

10.3.2 Da chi vogliamo difenderci?

I rischi studiati nell'esempio "una nuova partenza"[3] valgono anche qui: un furto, una perquisizione che abbia dei motivi che possono anche non essere direttamente legati alle informazioni che vogliamo proteggere.
Aggiungiamo a questi rischi la possibilità che il libro o il film prodotto non piaccia a qualche commissario, ministro, CEO, o simili. Può succedere. Poniamo che:

- questa autorità abbia avuto degli indizi che gli permettano di supporre chi sia l'autore del capolavoro;

2 Cap. 6
3 Cap. 8

- questa autorità sia in grado di disporre di una temibile squadra di uomini dotati di armi e uniformi, di poter agire la mattina presto e di sapere il domicilio delle persone sospettate.

Una tale inopportuna intrusione porterà, come minimo, in modo evidentemente anche fastidioso, al sequestro di tutto il materiale informatico che verrà trovato. Questo materiale verrà consegnato dagli intrusi nelle mani di qualcun altro di fiducia che metterà in pratica una specie di autopsia volta a riesumare i dati presenti... o che erano presenti in passato[4].

10.4 Possibili attacchi e soluzioni praticabili

Il metodo più semplice al momento è:

- creare una penna USB o un hard-disk cifrato[5];
- copiare i file da archiviare dentro questa periferica;
- eliminare e cancellare *davvero* il contenuto dei file di lavoro[6].

Una volta effettuate queste operazioni, la penna o l'hard-disk potranno essere riposti altrove rispetto al luogo dove utilizziamo normalmente il computer.
Si potrebbe anche studiare l'uso del CD o del DVD, per il loro basso costo, ma al momento è più complesso cifrare correttamente dei dati su questi supporti piuttosto che su delle penne USB, che sono ormai moneta corrente e facili da procurarsi.

4 Cap. 4.3
5 Cap. 18
6 Cap. 17

10.5 Quale password?

Dato che i file saranno salvati sotto forma cifrata, sarà necessario scegliere una password[7]. Ora, visto che la destinazione è l'archiviazione, questa password non verrà utilizzata frequentemente. E una password utilizzata di rado ha tutte le possibilità del mondo di essere dimenticata... rendendo in pratica impossibile l'accesso ai dati. Riguardo a questo problema, possiamo studiare qualche strada.

10.5.1 Scrivere la password da qualche parte

Tutta la difficoltà consiste nel sapere dove scriverla, mettere questo documento in un posto dove poi lo si può trovare... senza d'altra parte far sì che altri possano ritrovarlo e capire che si tratta di una password.

10.5.2 Utilizzare la stessa password del nostro sistema quotidiano

La password del nostro sistema quotidiano, nel caso in cui sia cifrato (vedi ricetta "installare un sistema cifrato")[8], è una password che usiamo regolarmente, e quindi ha tutte le possibilità di venire ricordata. Il rovescio della medaglia:

- se siamo costretti a rivelare la password del sistema, abbiamo rivelato anche quella dell'archivio;
- non bisogna avere una così grande fiducia nei computer attraverso i quali accederemo all'archivio. Potremmo farci beccare a nostra insaputa la password, che poi potreb-

7 Cap. 12
8 Cap. 15

be venire usata in seguito non solo per leggere le informazioni archiviate, ma a quel punto anche tutti i dati contenuti nel computer.

10.5.3 Dividere il segreto con altri

Possiamo dividere il segreto con altri (vedi ricetta "dividere un segreto"[9]). In questo modo bisogna riunire più persone per poter accedere all'archivio. Bisogna però ponderare la cosa: questo metodo implica complicare l'accesso agli indesiderati, ma anche ai desiderati.

10.6 Un hard-disk? Una penna? Varie penne?

A seconda delle scelte fatte precedentemente riguardo alla password, dobbiamo ora decidere quale supporto utilizzare, considerando che, sul piano tecnico, la cosa più semplice al momento è quella di avere una sola password per ciascun supporto.
Un hard-disk esterno può contenere più dati di una penna USB, e a volte si rende quindi necessario: per archiviare un progetto video, per esempio.
Archiviare vari progetti sullo stesso supporto permette di semplificare la cosa, ma diventa in questo modo difficile separare i progetti in base ai livelli di riservatezza che necessitano.
Oltretutto, così facendo, le persone possono accedere agli archivi di un progetto, ma anche a quelli degli altri, il che non è di solito consigliabile.
Poi, se la password è un segreto diviso, è meglio facilitare l'accesso alle persone che condividono il segreto avendo un supporto che possano trasmettersi.

---

9 Cap. 20

TERZA PARTE

Utensili

In questa parte della guida, spiegheremo come applicare nel concreto alcune delle strade a cui abbiamo accennato nelle puntate precedenti.
Si tratta di un'appendice tecnica alle precedenti: una volta comprese le problematiche legate all'intimità nel mondo digitale, una volta scelte le risposte adatte, resta la questione di "come fare?". Nei prossimi capitoli troverete alcune risposte a questa domanda.

Sul buon uso delle ricette
Gli strumenti e le ricette che seguono sono delle soluzioni estremamente parziali, che trovano un'utilità soltanto se unite a una serie di pratiche coerenti tra loro.
Pescare nella cassetta degli attrezzi senza avere prima studiato la parte sulla scelta delle risposte adatte[1] e senza aver definito una policy di sicurezza, è un buon modo per tirarsi la zappa sui piedi convinti – a torto – di aver risolto questo o quel problema.

Non si può piacere a tutti
Partiamo dal principio che, per la maggior parte delle ricette presentate in questa guida, utilizzeremo GNU/Linux con l'interfaccia GNOME. Le ricette sono state testate su Debian GNU/Linux versione 9.0 (Stretch) e Tails (*The Amnesic Incognito Live System*), ma sono generalmente compatibili anche con altre distribuzioni basate su Debian, come Ubuntu o Linux Mint.
Se ancora non utilizzate GNU/Linux, consultate l'esempio "una nuova partenza"[2] o la ricetta "utilizzare un sistema Live"[3].

---

1 Cfr. Seconda parte delal guida
2 Cap. 8
3 Cap. 14

Sulla buona interpretazione delle ricette
Prima di passare alle ricette vere e proprie, ci sembra necessario qualche avvertimento trasversale.
Nel caso di alcuni strumenti, le procedure sono presentate passo passo e quando possibile spiegano il senso delle azioni che vengono proposte. Un uso efficace di questi strumenti necessita di intendersi su alcuni punti:

- L'ordine nel quale ciascuna ricetta viene sviluppata è di importanza capitale. Salvo diversa indicazione, è semplicemente inimmaginabile saltare un passo per tornarci poi dopo; il risultato, sempre che le operazioni così disordinate ne dessero uno, potrebbe essere molto diverso da quello voluto, forse anche catastrofico.
- Per le stesse ragioni, le azioni indicate devono essere effettuate alla lettera. Omettere un'opzione, aprire la directory sbagliata, può modificare il senso o gli effetti di una ricetta.
- In generale la buona comprensione delle ricette richiede un minimo di attenzione e agilità mentale. Non possiamo rispiegare tutto ogni volta; daremo per scontato che siano state seguite e integrate le spiegazioni date nei precedenti "Esempi", di cui queste ricette non sono che l'ultimo passo.

Infine, queste pagine che avete tra le mani potrebbero non essere aggiornate con le versioni attuali dei software implicati. La versione online originale (in francese) potrebbe essere più aggiornata (https://guide.boum.org).

11 | Utilizzare un terminale

I software evolvono, per questo è vivamente consigliato utilizzare la versione più aggiornata di questa ricetta, che troverete in francese e in italiano sui siti della Guida https://guide.boum.org/ e https://numerique.noblogs.org/.

Durata: dai 15 ai 30 minuti.

Generalmente usiamo il computer cliccando su dei menu e delle icone. Ma esiste un altro modo per "parlargli": digitando delle righe di testo che si chiamano "comandi". Questa maniera di interagire con un computer si chiama "terminale" o "shell" o ancora "riga di comando".
Questa guida cerca di limitare il più possibile l'uso di questo strumento, che è abbastanza spaesante per chi non è abituato. Nonostante ciò, a volte è indispensabile servirsene.

11.1 Che cos'è un terminale?

Spiegare nel dettaglio l'uso della riga di comando non è lo scopo di questa guida, e internet straripa di tutorial e corsi che assolvono molto bene questo compito. Ci sembra però comunque necessario gettare un po' di basi sul modo in cui servirsene.
Bene, prima di tutto cominciamo aprendo semplicemente un terminale: nell'ambiente grafico GNOME 3, bisogna aprire la vista d'insieme delle attività premendo il tasto ⊞ (⌘ su Mac), poi digitare `term` e cliccare su "Terminale".
A questo punto apparirà una finestra che indica:

```
utente@nomedelcomputer: ~$
```

Alla fine c'è un quadratino, chiamato "cursore", che indica dove scrivere il testo del comando.
Per esempio, usando l'utente "roger" su una macchina chiamata "debian", ci ritroveremo:

```
roger@debian: ~$
```

A partire da questo punto, chiamato "prompt", possiamo scrivere direttamente i comandi che vogliamo far eseguire al computer.
Il risultato finale di questi comandi è spesso lo stesso di quello che potevamo ottenere cliccando nel posto giusto all'interno di un'interfaccia grafica. Per esempio, se una volta aperto il terminale scriviamo

```
gedit
```

e poi premiamo Invio, il risultato sarà quello di aprire un editor di testo. Avremmo potuto fare la stessa cosa premendo il tasto ⊞ (⌘ su Mac), scrivendo `testo` e poi cliccando su "gedit".
Di contro, non potremo inserire un nuovo comando nel nostro terminale finché non usciremo dall'editor di testo.
Nel quadro di questa guida, il terminale ci serve soltanto per compiere quelle azioni che al momento non hanno un'alternativa grafica.

11.2 I comandi

I comandi sono ordini che impartiamo al computer attraverso il terminale. Queste "righe di comando" hanno il proprio linguaggio, con le loro parole, le loro lettere e la loro sintassi. Quindi occorre fornire qualche avvertenza in questo senso.

11.2.1 Sintassi

Prendiamo per esempio il comando `sfill`, che permette pressappoco le stesse operazioni di `nautilus-wipe`, un programma grafico che presenteremo più avanti[1]:

```
sfill l v /home
```

In questa riga di comando vediamo, nell'ordine:

- il comando che si chiama `sfill`. Il comando in genere è un programma installato sul sistema;
- due opzioni, `-l` e `-v`, che modificano il comportamento del programma `sfill`. Queste ultime possono essere facoltative a seconda del programma (e iniziare con un trattino o due per distinguerle);
- un argomento `/home` che precisa su cosa deve agire il comando. Possono essercene molti o nessuno, dipende sempre dal comando.

Ciascuno di questi elementi deve essere separato dagli altri da uno o più spazi. Quindi c'è uno spazio tra il comando e la prima opzione, tra la prima opzione e la seguente, tra l'ultima opzione e il primo argomento, tra il primo argomento e i seguenti…
Per conoscere le opzioni e gli argomenti di un comando non ci sono segreti: ciascun comando prevede normalmente una pagina di manuale. Per accedervi basta scrivere nel terminale `man` seguito dal nome del comando e poi premere invio.
I manuali spesso però possono essere difficili da comprendere per i loro aspetti tecnici e a volte sono disponibili solo in lingua inglese.

---

1 Cap. 17.7

11.2.2 Inserimento del percorso (path)

Durante l'utilizzo del terminale, avremo spesso bisogno di indicare cartelle e file. La cartella o la sottocartella in cui si trova il file si chiama "percorso". Per differenziare una cartella da ciò che contiene, si utilizza il carattere `/` (che si pronuncia "slash").
Per fare un esempio, ecco il percorso del documento `ricetta.txt` che si trova nella cartella `Documenti` della home personale dell'utente chiamato `alligatore`:

```
/home/alligatore/Documenti/ricetta.txt
```

Siccome molti comandi si aspettano dei nomi di file come argomento, diventa presto fastidioso scrivere ogni volta a mano il loro percorso. Quindi c'è un modo semplice per inserire un percorso: se prendiamo l'icona di un file con il mouse e la trasciniamo dentro il terminale, il suo percorso viene scritto nel punto in cui si trova il cursore.
Questo metodo funziona però soltanto con i file e cartelle veri e propri. Per esempio, con i file messi dentro al Cestino otterremo un nome bizzarro che non funzionerà, stessa cosa per l'icona della home sulla Scrivania o per l'icona della penna USB.

11.2.3 Esecuzione

Una volta che si scrive un comando, si chiede al computer di "eseguirlo" premendo il tasto Invio.

11.2.4 Fine o interruzione del comando

L'esecuzione del comando può impiegare più o meno tempo.

Quando finisce, il terminale torna sempre allo stato in cui si trovava prima di aver lanciato il comando, il *prompt*:

```
roger@debian: ~$
```

In questo caso si dice che il terminale "restituisce il prompt".
Se abbiamo bisogno di interrompere l'esecuzione di un comando prima che sia terminato, dobbiamo premere *ctrl+c* (il tasto *ctrl* unito al tasto *c*). In questo modo si stoppa il comando immediatamente, un po' come si fa quando si chiude la finestra di un programma.

11.3 Permessi d'amministrazione

Alcuni comandi che modificano il sistema necessitano dei diritti di amministrazione. In questo modo è possibile accedere integralmente al sistema, senza restrizioni… con i rischi che ciò comporta.
Per eseguire un comando con i diritti di amministrazione, bisogna scrivere `pkexec` prima del comando. Si aprirà una finestra che ci chiederà la password prima di eseguire il comando.

11.4 Un altro avvertimento

Sopratutto per le ricette di cui parleremo dopo, i comandi devono essere scritti molto precisamente. Dimenticare uno spazio, omettere un'opzione, dimenticarsi di un carattere, essere imprecisi su un argomento, vuol dire cambiare significato al comando.
E siccome il computer compie *esattamente* ciò che gli si dice di fare, se cambiamo il comando, farà *esattamente altre cose…*

11.5 Un esercizio

Creiamo un file vuoto chiamato "prova", che poi cancelleremo. In un terminale, scriviamo il comando:

```
touch prova
```

e diamo invio per farlo eseguire al computer. Il comando `touch` dà l'ordine al computer di creare un file vuoto; l'argomento prova indica il nome di questo file. In questo caso non sono state utilizzate opzioni.
Verifichiamo poi che questo file sia stato effettivamente creato, lanciando il comando `ls` (che significa lista):

```
ls
```

Una volta lanciato il comando, il computer risponde con una lista. In questo caso eccola:

```
Documenti prova
```

`Documenti` è il nome di una cartella che esisteva anche prima, e `prova` è il nome del file che abbiamo appena creato. Un altro computer avrebbe potuto rispondere con tanti altri file oltre a `Documenti` e `prova`.

Il risultato di `ls` non è che un altro modo di vedere ciò che si poteva ottenere anche in altro modo. Se si clicca sulla Scrivania, sull'icona della cartella personale, vedremo che è comparsa una nuova icona che rappresenta il file di prova, che abbiamo appena creato.
Adesso cancelliamo questo file. La riga di comando per farlo ha questa sintassi generale:

```
rm opzioni nome_del_file_da_cancellare
```

Utilizziamo l'opzione `-v`, che nel contesto di questo comando, serve a chiedere al computer di essere più verboso (mostrare più dettagli) riguardo alle azioni che compirà.
Per inserire il nome del file da cancellare, usiamo il trucchetto di prima per indicare il percorso di un file. Quindi:

- scriviamo `rm -v` nel nostro terminale;
- aggiungiamo uno spazio dopo `-v` per separare l'opzione dal resto;
- nella finestra della cartella personale, prendiamo con il mouse l'icona del `file` e la trasciniamo nel terminale.

Alla fine di questa operazione dovremmo ottenere qualcosa come:

```
rm -v '/home/LOGIN/prova'
```

Possiamo allora dare Invio e osservare che il computer risponderà:

```
"/home/LOGIN/prova" rimosso
```

Quindi il file è stato cancellato. Possiamo ancora una volta verificarlo lanciando di nuovo `ls`:

```
W
```

e noteremo l'assenza del file prova. Allo stesso tempo anche l'icona sarà sparita. A prima vista il file è stato cancellato... anche se, come abbiamo spiegato nella prima parte[2], il suo

2 Cap. 4.3

contenuto esiste ancora sul disco. Siccome in questo caso il file prova era vuoto, possiamo ritenerlo un fatto non troppo grave.

11.6 Attenzione alle tracce!

La maggior parte delle shell salvano automaticamente[3] le righe di comando che abbiamo digitato, all'interno di un file con lo storico. Questa cosa è pratica per poter ritrovare in seguito i comandi che abbiamo utilizzato, ma lascia anche una traccia delle nostre attività.
La shell standard di Debian si chiama `bash`. In quest'ultima, per disattivare temporaneamente il salvataggio dello storico nel terminale che stiamo utilizzando, basta fare:

```
unset HISTFILE
```

Altrimenti, i comandi verranno salvati nel file nascosto `bash_history` (che si trova dentro la home personale). Potrebbe essere una buona idea quella di ripulirlo[4] di tanto in tanto.

11.7 Per andare oltre

Questa prima esperienza con questa finestra piena di piccoli caratteri potrebbe essere l'inizio di una passione duratura. Per coltivarla, non c'è niente di meglio che prendersi il tempo di leggere qualche "howto": *http://rofifo.vado.li/*

3 Cap. 2.5
4 Cap. 17.4

12 | Scegliere una passphrase

I software evolvono, per questo è vivamente consigliato utilizzare la versione più aggiornata di questa ricetta, che troverete in francese e in italiano sui siti della Guida https://guide.boum.org/ e https://numerique.noblogs.org/

Durata: circa 10 minuti.

Una passphrase è un segreto che serve a proteggere dei dati cifrati. È ciò che si utilizza per cifrare un hard-disk, delle e-mail, dei documenti... oppure, come vedremo nei capitoli della guida che seguiranno, delle chiavi crittografiche.
Parliamo di "passphrase", anziché di "password", perché una sola parola, per quando bizzarra e complicata, è molto meno resistente rispetto a una semplice frase composta da varie parole. Una passphrase dovrebbe contenere almeno dieci parole. Ma più ce ne mettiamo meglio è!
Un criterio importante, ma a volte trascurato: una buona passphrase è una frase che possiamo *ricordarci*[1], in questo modo evitiamo di dovercela annotare su carta, grave errore che vanifica una passphrase anche granitica. Inoltre, altrettanto importante, una buona passphrase deve essere il più difficile possibile da indovinare. Evitiamo quindi passphrase formate da 15 parole di caratteri casuali che ci dimenticheremo dopo un quarto d'ora, ma non scegliamo neanche titoli delle più famose hit trash anni 80.
Una tecnica semplice per trovare una buona passphrase, difficile da indovinare, ma anche facile da ricordare, è quella di costruire una frase che non derivi da un testo già esistente. Con le parole di una canzone, il versi di una poesia, la citazione di

1 Randall Munroe, 2014, *Password Strength* [http://sigipa.vado.li/].

un libro, esistono degli strumenti come il progetto *Gutenberg*[2] che rendono sempre più facile testare le passphrase derivate dalla letteratura esistente[3].
Anche nel caso in cui vogliate utilizzare la vostra immaginazione, possiamo darvi dei consigli riguardo alla scelta di una password.

1. Pensiamo innanzitutto a una frase che non ci scorderemo facilmente. Spremiamoci le meningi un istante.
2. Cerchiamo all'interno di questa frase cosa possiamo modificare per renderla più difficile da indovinare. Possiamo per esempio aggiungere del dialetto, delle parole in altre lingue, mettere delle maiuscole qua e là dove uno non se le aspetterebbe, rimpiazzare dei caratteri con altri, interpretare liberamente l'ortografia, ecc.

Però un consiglio: è meglio evitare i caratteri accentati o altri simboli che non sono direttamente disponibili su una tastiera americana. Questo per evitare problemi di tasti assenti o difficili da trovare, e soprattutto per evitare una codifica sbagliata dei caratteri, nel caso in cui dovessimo trovarci a digitare la nostra passphrase con una tastiera diversa da quella a cui siamo abituati. Per esempio, prendiamo questa frase che apparentemente non ha senso:

corretto cavallo pila disgrafica

Possiamo trasformarla così, per ottenere una passphrase migliore:

koretto cabalLo-pEela! disGraffica

---

2 Wikipedia, 2019, Progetto *Gutenberg* [http://dudebi.vado.li/].

3 Dan Goodin, 2013, *How the Bible and YouTube are fueling the next frontier of password cracking* [http://zinibi.vado.li/].

Una volta creata la vostra passphrase, può essere una buona idea quella di utilizzarla subito per una dozzina di volte per decifrare i vostri dati. Questo vi permetterà di fare imparare alle vostre dita come digitarla e di memorizzarla mentalmente e fisicamente.
Non dimentichiamo però che se ci siamo sforzati di trovare una buona passphrase, questo non ci dispensa dal doverne trovare un'altra per un supporto cifrato differente. L'uso della stessa passphrase, o peggio della stessa password, per una varietà di cose diverse, caselle mail, conti Paypal, conti bancari online, ecc. può rivelarsi una scelta disastrosa nel caso in cui venga violata. Per esempio se il servizio di conto bancario online si è fatto compromettere.

13 | Avviare da CD, DVD o penna USB

Durata: da 1 a 20 minuti circa.

Adesso vediamo come far avviare un PC da un dispositivo esterno, per esempio un CD di installazione di Debian, o un sistema Live su una penna USB.
A volte, soprattutto sui computer moderni, è molto semplice. Altre volte c'è un po' da strapparsi i capelli… Dipende tutto dalla parte iniziale della procedura di avvio del computer, dal firmware[1]. Come abbiamo visto, il firmware è ciò che permette di scegliere la periferica (hard-disk, penna USB, CD-ROM, ecc.) dove si trova il sistema che vogliamo utilizzare.

13.1 Provare e basta

Cominciamo con l'inserire il CD o il DVD nel lettore, o attaccando la penna USB, poi (ri)avviamo il computer. A volte funziona da solo alla prima. Se è così, abbiamo vinto, non importa leggere il resto.

13.2 Provare a scegliere la periferica d'avvio

Nei firmware recenti, spesso è possibile scegliere di volta in volta la periferica dalla quale si vuole avviare. Ma non è sempre possibile, soprattutto per alcuni computer recenti dotati di Windows 10, nei quali invece la scelta è resa più complicata. Tra le altre cose toccherà disattivare il Secure boot e cercare sul web come far avviare da una penna USB quel par-

1 Cap. 1.2.6

ticolare modello di computer. (Ri)avviare il computer facendo molta attenzione a tutti i primi messaggi che compaiono sullo schermo. Cercare quei messaggi in inglese che assomigliano a qualcosa del tipo:

- `Press [KEY] to select temporary boot device`
- `[KEY] = Boot menu`
- `[KEY] to enter MultiBoot Selection Menu`

Questi messaggi indicano di utilizzare il tasto KEY per scegliere una periferica da cui fare il boot (l'avvio). Questo tasto spesso è F2 o F9 o ESC.
Sui Mac, c'è un equivalente di questa opzione: subito dopo l'accensione del computer, tenere premuto il tasto ALT. Nel giro di poco dovremmo veder apparire le opzioni di boot.
Ma torniamo al nostro PC. Spesso il firmware va troppo veloce e non abbiamo il tempo di leggere il messaggio, di capirlo e premere il tasto giusto. Una volta individuato il tasto giusto, riavviamo e premiamolo (non tenendo premuto, ma premendo e ripremendo molte volte) non appena il computer si accende. Con un po' di fortuna otterremo un messaggio tipo questo:

```
            Boot Menu
-----------------------------------
 1:  USB HDD
 4:  IDE HDD0: BDS GH87766319819
 8:  Legacy Floppy Drives

          <Enter Setup>
```

Se questa cosa ha funzionato, abbiamo vinto. Scegliamo l'opzione giusta nel menu, spostandosi in alto e in basso con le frecce ↑ e ↓ della tastiera, e poi diamo Invio. Per esempio, per

avviare da penna USB, scegliere USB HDD. In questo modo il computer si avvierà dalla periferica selezionata. Se ha funzionato, saltate le prossime parti.

13.3 Modificare i parametri del firmware

Se scegliere una periferica di avvio temporaneo non funziona, bisogna rientrare nel BIOS per scegliere la sequenza di boot a mano. Tanto per mettere un po' di pepe, i firmware sono quasi tutti diversi tra loro, in modo che sia impossibile per noi indicarvi un metodo che funzioni ogni volta[2].

13.3.1 Entrare nel BIOS

Bisogna ancora una volta (ri)avviare il computer e osservare attentamente i primi messaggi che appaiono. Cerchiamo i messaggi che assomigliano a qualcosa come:

- `Press [KEY] to enter setup`
- `Setup: [KEY]`
- `[KEY] = Setup`
- `Enter BIOS by pressing [KEY]`
- `Press [KEY] to enter BIOS setup`
- `Press [KEY] to access BIOS`
- `Press [KEY] to access system configuration`
- `For setup hit [KEY]`

Questi messaggi indicano di premere il tasto KEY per entrare nel BIOS. Questo tasto è spesso Del (Canc) o F2, a volte F1, F10, F12, Esc, Tab o altro ancora.

2 A questo indirizzo trovate dei tutorial illustrati per alcuni BIOS: http://dogufe.vado.li/

Ecco qua sotto una tabella che riassume i tasti per accedere al BIOS, almeno per alcune delle ditte costruttrici più comuni[3].

Azienda	**Tasto**
Acer	F1, F2, DEL
Compaq	F10
Dell	F2
Fujitsu	F2
HP	F1, F2, F10, F12, ESC
IBM	F1
Lenovo	F1
NEC	F2
Packard Bell	F1, F2, DEL
Samsung	F2
Sony	F1, F2, F3
Toshiba	F1, F2, F12, ESC

Spesso il firmware va troppo veloce e non abbiamo il tempo sufficiente per leggere il messaggio, capirlo e premere il tasto giusto. Una volta individuato il tasto giusto, riavviamo e premiamolo (non tenendo premuto, ma premendo e ripremendo tante volte) non appena il computer si accende. A volte il computer si perde e si pianta. In questo caso, spegniamo e riproviamo da capo.
Se invece del messaggio che speravamo di vedere, appare un'immagine fissa, può darsi che il BIOS sia configurato per

3 Tim Fisher, 2014, *BIOS Setup Utility Access Keys for Popular Computer Systems* [http://bacosu.vado.li/], o anche MichaelStevensTech, 2014, *How to access/enter Motherboard BIOS* [http://lanona.vado.li/].

far visualizzare un logo al posto dei messaggi. Proviamo a premere il tasto Esc o Tab.
Se il computer parte troppo velocemente e non abbiamo il tempo di leggere i messaggi che ci fa vedere, a volte può funzionare premere il tasto Pausa (spesso in alto a destra nella tastiera) per bloccare lo schermo. Per riattivarlo, premere un tasto qualsiasi.

13.3.2 Modificare la sequenza di boot

Una volta entrati nel BIOS, ci troveremo davanti una schermata generalmente blu o nera, piena di menu. Di base ci sarà una zona in basso o a destra dello schermo che spiega come spostarsi tra le opzioni, come selezionare gli elementi, come cambiare menu, ecc.

Quello che bisogna fare è cercare un po' ovunque, finché non si trova qualcosa che contiene la parola "boot" e che assomiglia a qualcosa del tipo:

- `First Boot Device Boot Order`
- `Boot Management Boot Sequence`

Se non troviamo niente, cerchiamo qualcosa come “Advanced BIOS Features” (negli AwardBIOS) o “Advanced features” (negli AMIBIOS).
Una volta trovato il menu giusto, si tratta di capire come si fa a modificarlo. Per esempio `Enter: Select` o `+/-: Value`.
L’obiettivo è quello di mettere il CD/DVD o l’USB al primo posto, a seconda di quello che ci serve.
A volte occorre entrare in un sottomenu, come nel caso in cui ci sia un menu Boot order, altre volte le opzioni si cambiano direttamente.

13.3.3 Scegliere bene la nuova configurazione

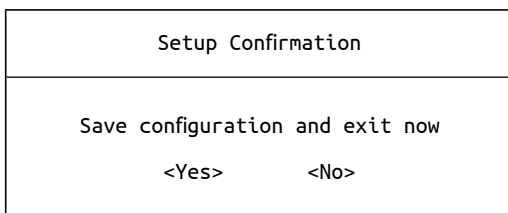
Una volta che siamo riusciti a selezionare il supporto giusto per l’avvio, dobbiamo domandarci se vogliamo che resti così per sempre o no. Se vogliamo lasciarlo così, potrebbe essere utile mettere l’hard-disk al secondo posto nella sequenza di boot. In questo modo, nel caso in cui il supporto al primo posto non ci sia, il computer farà il normale boot da hard-disk. Se non mettiamo l’hard-disk nella sequenza di boot, il computer – non trovando un CD, un DVD, o una penna USB – non si avvierà proprio.
D’altra parte lasciare sempre che il computer possa avviarsi da un supporto esterno potrebbe avere delle conseguenze inopportune: per un intruso sarebbe più semplice fargli fare il boot da un proprio supporto.
Certo possiamo mettere una password al BIOS. Ma è inutile farci affidamento perché ci protegga: questo tipo di protezione può essere aggirata molto facilmente.

13.3.4 Salvare e uscire

Una volta che abbiamo deciso la nuova configurazione, non resta che salvare e uscire. Per farlo leggiamo ancora una volta gli aiuti che compaiono sullo schermo, per esempio qualcosa come `F10: Save`. A volte bisogna premere Esc un po' di volte per arrivare al menu giusto. A quel punto ci apparirà un messaggio che ci chiederà se siamo sicuri di voler salvare e uscire.

```
Setup Confirmation

Save configuration and exit now

<Yes>       <No>
```

Vogliamo effettivamente salvare, quindi selezioniamo "Yes" e premiamo Invio.

14 | Utilizzare un sistema Live

I software evolvono, per questo è vivamente consigliato utilizzare la versione più aggiornata di questa ricetta, che troverete in francese e in italiano sui siti della Guida https://guide.boum.org/ e https://numerique.noblogs.org/.

Durata: da mezz'ora a un'ora + mezz'ora circa per il download.

Un sistema Live è un sistema GNU/Linux che funziona senza essere installato sull'hard-disk del computer.
Attenzione, questo non significa che non verranno lasciate tracce sull'hard-disk: per esempio, molti sistemi Live utilizzano la swap[1]. A volte usano in automatico anche le partizioni che trovano.

14.1 I sistemi Live discreti

Alcuni sistemi Live invece sono pensati specialmente per (provare a) non lasciare alcuna traccia sull'hard-disk, salvo quando non gli si chieda esplicitamente di farlo. Questo è il caso di Tails (*The Amnesic Incognito Live System*).
In questo caso (se chi ha sviluppato il sistema Live non ha sbagliato) non verrà scritto niente sull'hard-disk. Tutto ciò che verrà fatto a partire dal sistema Live sarà scritto soltanto nella RAM[2], che si cancella da sola più o meno per davvero quando spegniamo il computer, almeno dopo un po'. Usare un sistema Live del genere quindi è uno dei migliori modi per usare un computer senza lasciare tracce.

1 Cap. 1.5.4
2 Cap. 1.2.3

Vedremo adesso insieme come procurarsi un sistema Live e come farlo avviare.
Il modo più diffuso di utilizzare un sistema Live è quello di installarlo su una penna USB o di masterizzarlo su un DVD.
Generalmente viene consigliato di utilizzare Tails su una penna USB: questo consente di servirsi di alcune funzionalità che non sono disponibili sul DVD, come gli aggiornamenti automatici e la persistenza.
Ma è anche vero che su una penna USB è possibile scrivere dati, cosa che invece non si può fare su un DVD, il che vuol dire che dei malintenzionati potrebbero modificare il vostro sistema Live, facendogli salvare, per esempio, le vostre password o ciò che avete digitato. Se per questa ragione scegliamo di usare un DVD, non dimentichiamo di fare gli aggiornamenti manualmente, a meno di non voler utilizzare un sistema che contenga delle note falle di sicurezza[3]!

14.2 Scaricare e installare Tails

Adesso spieghiamo come scaricare l'ultima versione di Tails dal sito ufficiale, come verificarne l'autenticità e come installarla su una penna USB o masterizzarla su un DVD.
Se già disponiamo di un'installazione dell'ultima versione di Tails, possiamo semplicemente clonarla. Saltate a più avanti per vedere come[4].
Per scaricare e installare Tails, utilizziamo la procedura guidata ufficiale, disponibile alla pagina `tails.boum.org/install/index.it.html`

⚠ *Attenzione*: questa guida fornisce delle spiegazioni su come verificare l'autenticità di un'immagine di Tails. Quando

3 Cap. 3.2
4 Cap. 14.3

nel corso della procedura vedremo “Verifica immagine ISO” possiamo usare questi consigli per verificare la sua autenticità.

14.2.1 Scaricare Tails

Tails può essere scaricata in due maniere: direttamente via web, tramite un browser, oppure con l’aiuto di BitTorrent.
In entrambi i casi dovremo servirci della procedura guidata di Tails relativa al sistema operativo che stiamo usando.

Download diretto
Se abbiamo scelto di scaricare l’immagine direttamente con il browser, dobbiamo come prima cosa installare il plugin di Firefox che permette di verificare l’integrità di Tails. Una volta scaricata l’immagine, se vogliamo spingerci oltre nella verifica dell’immagine ISO e allo stesso tempo assicurarci della sua autenticità, dobbiamo cliccare sulla firma OpenPGP e seguire le istruzioni corrispondenti.

Download via Torrent
Se abbiamo scelto di scaricare l’immagine via BitTorrent, il download conterrà sia l’immagine ISO che la firma che permette di verificarne l’autenticità.

14.2.2 Verificare l’autenticità di un sistema Live

L’estensione del browser per la verifica di Tails effettua una prima verifica dell’immagine scaricata. Questa verifica garantisce soprattutto che l’immagine corrisponda a quella distribuita dal sito di Tails[5], ma non ci protegge nel caso in

5 Il modello di rischio al quale risponde il plugin per il download di Tails è documentato sul sito di Tails [http://vocale.vado.li/].

cui fosse stato attaccato il sito. L'immagine del sistema Live che abbiamo scaricato è firmata digitalmente con OpenPGP. Utilizzeremo questa firma per verificare in modo più robusto l'autenticità dell'immagine scaricata.
Cominciamo con l'importare la chiave OpenPGP che firma le ISO di Tails:

```
Tails developers
tails@boum.org 'offline long-term identity key'
```

Poi verifichiamo la firma digitale dell'immagine ISO. Questa è la fingerprint che gli autori di questa guida hanno osservato, posto che quello che avessero tra le mani fosse una copia originale:

```
A490 D0F4 D311 A415 3E2B B7CA DBB8 02B2 58AC D84F
```

14.2.3 Installare Tails sul dispositivo scelto

Ritorniamo alla procedura guidata di Tails e andiamo alle istruzioni corrispondenti al nostro sistema operativo per l'installazione di Tails su una penna USB. Se invece vogliamo installare Tails su un DVD, andiamo a quella pagina.

14.3 Clonare o aggiornare una penna Tails

Una volta che disponiamo di un DVD o di una penna USB con sopra Tails, è possibile duplicarla, per esempio per creare una penna USB con la persistenza corrispondente a una nuova identità contestuale, oppure per regalare una penna Tails a qualcuno, o ancora per aggiornare una penna USB contenente una vecchia versione di Tails.

Per fare ciò, seguiamo la documentazione ufficiale di Tails, che è disponibile su tutti i DVD o penne USB di Tails, anche offline.
Avviamo Tails. Sulla Scrivania, clicchiamo sull'icona "Documentazione di Tails". Nel menu a destra, clicchiamo su "Documentazione". Nell'indice che si aprirà, cerchiamo la sezione "Download e installazione" e clicchiamo sulla pagina "Installazione a partire da un'altra Tails". Sono queste le istruzioni che dovremo seguire.
Per aggiornare una penna creata in precedenza, bisogna invece seguire la pagina "Aggiornare una penna USB o una scheda SD Tails" nella sezione "Primi passi con Tails".

14.4 Avviare da un sistema Live

Quando la copia o la masterizzazione è terminata, possiamo riavviare il computer lasciandoci attaccato (o dentro) il supporto del sistema Live e verificare che la copia abbia funzionato... a condizione, ovviamente, che abbiamo prima configurato il BIOS in modo che faccia partire il supporto giusto[6].
All'avvio, Tails mostra una schermata che permette di scegliere, tra le altre opzioni, la lingua e la disposizione della tastiera.

14.5 Utilizzare la persistenza di Tails

Quando utilizziamo Tails su una penna USB, possiamo creare un volume persistente cifrato sullo spazio libero della penna creato con l'installer di Tails.
I dati persistenti contenuti nel volume vengono salvati e resta-

6 Cap. 13

no disponibili tra un uso di Tails e l'altro. Il volume persistente permette di salvare file personali, chiavi crittografiche, configurazioni o software che non sono installati di default su Tails. Una volta creato il volume persistente, a ciascun avvio di Tails possiamo scegliere se attivarlo o no[7].
Potremo poi decidere di cancellarlo quando non vorremmo più avere accesso a quei dati[8]. L'utilizzo di un volume persistente però non è privo di conseguenze rispetto alle tracce lasciate in giro. Per questo occorre leggere bene la pagina delle avvertenze sull'uso della persistenza.
Clicchiamo sull'icona "Documentazione di Tails" che si trova sulla Scrivania. Nel menu a destra, clicchiamo su "Documentazione". Nell'indice che si aprirà, cerchiamo la sezione "Primi passi con Tails" e clicchiamo sulla pagina "Avvertenze riguardo alla persistenza".

14.5.1 Creare e configurare un volume persistente

Per creare e configurare un volume persistente su una penna USB Tails, basta seguire la documentazione ufficiale di Tails, disponibile su tutte le penne USB o DVD di Tails, anche offline.
Avviamo Tails[9]. Clicchiamo sull'icona "Documentazione di Tails" che si trova sulla Scrivania. Nel menu a destra, clicchiamo su "Documentazione". Nell'indice che si aprirà, cerchiamo la sezione "Primi passi con Tails" e clicchiamo sulla pagina "Creare e configurare il volume persistente".
Se abbiamo già un volume persistente e vogliamo semplicemente modificarne i parametri, andiamo direttamente alla sezione "Opzioni della persistenza".

7 Cap. 14.5.2
8 Cap. 14.5.3
9 Cap. 14.4

14.5.2 Attivare e utilizzare un volume persistente

Per attivare il volume persistente appena creato su una penna USB di Tails, seguiamo ancora la documentazione ufficiale di Tails, disponibile su tutte le penne USB o DVD di Tails, anche offline.
Avviamo Tails[10]. Clicchiamo sull'icona "Documentazione di Tails" che si trova sulla Scrivania. Nel menu a destra, clicchiamo su "Documentazione". Nell'indice che si aprirà, cerchiamo la sezione "Primi passi con Tails", clicchiamo sulla pagina "Persistenza" e infine "Attivare e utilizzare il volume persistente".

14.5.3 Cancellare un volume persistente

Per cancellare un volume persistente creato in precedenza su una penna USB di Tails, seguiamo la documentazione ufficiale di Tails, disponibile su tutte le penne USB o DVD di Tails, anche offline.
Avviamo Tails[11]. Clicchiamo sull'icona "Documentazione di Tails" che si trova sulla Scrivania. Nel menu a destra, clicchiamo su "Documentazione". Nell'indice che si aprirà, cerchiamo la sezione "Primi passi con Tails", clicchiamo su "Cancellare il volume persistente".

14.5.4 Installare un software aggiuntivo persistente in Tails

Tails contiene dei programmi adatti alla maggior parte degli utilizzi correnti per chi deve usare internet e creare documen-

10 Cap. 14.4
11 *ibidem*

ti. Nonostante ciò, per dei progetti specifici, potremmo aver bisogno di installare un software specifico dentro Tails, come ad esempio un software per disegnare e simulare circuiti elettronici.
Quando Tails è installata su una penna USB, possiamo configurare un volume persistente in modo che ad ogni avvio venga installato automaticamente uno o più software.

Trovare il nome del pacchetto da installare
Abbiamo bisogno del nome esatto del pacchetto da installare. Per trovarlo, seguire la ricetta su come trovare un software[12]. Per esempio, il nostro programma per disegnare circuiti elettrici è fornito dal pacchetto `geda`.

Configurare i software aggiuntivi
Per prima cosa dobbiamo seguire la ricetta precedente "Creare e configurare un volume persistente in Tails"[13] per attivare le opzioni "Pacchetti APT" e "Liste APT".
A questo punto riavviamo Tails. Una volta riavviato, al momento della schermata iniziale, dopo aver scelto la lingua, inseriamo la passphrase del volume persistente nella sezione "Volume persistente cifrato" e poi clicchiamo su "Sbloccare". Poi clicchiamo sul "+" posto sotto la voce "Parametri avanzati", poi clicchiamo su "Password di amministrazione", inseriamola due volte e clicchiamo su "Aggiungi". Infine clicchiamo su "Avviare Tails".
Una volta sulla Scrivania, apriamo un terminale root partendo dalla veduta d'insieme delle Attività che si ottiene premendo il tasto ⊞ (⌘su Mac),.
Inseriamo la password scelta prima e diamo Invio. Nel terminale che apparirà scriviamo:

12 Cap. 16.1
13 Cap. 14.5.1

```
gedit /live/persistence/TailsData_unlocked/live-additio-
nal-software.conf
```

e diamo invio. Si aprirà un file di testo. Ogni riga di questo file deve contenere il nome esatto di un pacchetto da installare. Aggiungiamo quindi una riga con il nome del pacchetto che abbiamo trovato prima. Nel nostro esempio scriveremo:

```
geda
```

Salviamo il file cliccando su Salva. Adesso possiamo chiudere il file di testo insieme al terminale e riavviare Tails. Ogni volta che attiveremo la persistenza e il computer sarà connesso alla rete, il nostro software verrà installato automaticamente impiegando un tempo più o meno lungo a seconda della grandezza e del numero dei software da installare (una finestra ci segnalerà che l'installazione è andata a buon fine).

15 | Installare un sistema cifrato

I software evolvono, per questo è vivamente consigliato utilizzare la versione più aggiornata di questa ricetta, che troverete in francese e in italiano sui siti della Guida https://guide.boum.org/ e https://numerique.noblogs.org/.

Durata: mettete in conto una giornata, con molti momenti d'attesa (a volte lunghi).

Abbiamo visto che tutti i computer, tranne quelli con alcuni sistemi Live, lasciano ovunque tracce dei file aperti[1], dei lavori effettuati, delle connessioni internet, ecc. Abbiamo anche visto che un modo per esporre un po' di meno i dati conservati sul computer è quello di cifrare in toto il sistema sul quale lavoriamo[2].
Quello che possiamo fare è installare un sistema operativo GNU/Linux come Debian o Ubuntu, su una partizione cifrata dell'hard-disk. Ad ogni avvio il computer ci chiederà una passphrase per sbloccare la decifratura del disco, dopodiché permetterà l'accesso ai dati e l'avvio del sistema. Senza quella passphrase, chiunque voglia accedere al contenuto di quel disco si troverà di fronte a dei dati indecifrabili.
Questo è ciò che faremo con questa ricetta.

15.1 Limiti

Attenzione: questa installazione cifrata semplice non risolve tutti i problemi di confidenzialità con un colpo di bacchetta. Protegge i dati solo in determinate condizioni.

1 Cap. 2
2 Cap. 5

15.1.1 Limiti di un sistema cifrato

Vi raccomandiamo caldamente queste letture preliminari:

- il capitolo che riguarda la cifratura (e i suoi limiti)[3];
- il caso di studio "una nuova partenza"[4], che affronta nel dettaglio i limiti pratici di questo tipo di sistema e gli attacchi possibili.

Ignorando questi limiti, l'installazione di un sistema cifrato può generare un falso senso di sicurezza, fonte di grossi problemi.

15.1.2 Limiti di una nuova installazione

Quando si installa un nuovo sistema, si parte da zero. Non c'è alcun modo semplice di verificare che il CD d'installazione che stiamo utilizzando sia affidabile e non contenga per esempio dei software malevoli. Potremo accorgercene in seguito, ma potrebbe essere troppo tardi.

15.1.3 Limiti nel riconoscimento dell'hardware

Utilizzare un sistema operativo libero come Debian ha uno svantaggio: i costruttori di componenti hardware ci fanno generalmente poca attenzione. A volte potrebbe essere difficile, o anche impossibile, utilizzare un computer o una delle sue periferiche sotto Debian[5].
La situazione negli ultimi anni sta migliorando: il riconosci-

---

3 Cap. 5
4 Cap. 8
5 Cap. 1.2.5

mento dell'hardware tende a essere più omogeneo, e soprattutto, la diffusione dei sistemi liberi sta spingendo sempre di più i costruttori a fare in modo, direttamente o indirettamente, che i propri componenti vengano riconosciuti[6].
Nonostante ciò, prima di sostituire un sistema operativo, potrebbe essere una buona idea accertarsi che i componenti hardware necessari funzionino bene, con l'aiuto di un sistema Live[7]. Il sistema Tails, per esempio, è basato su Debian. I componenti che funzionano con l'uno funzioneranno senza difficoltà anche con l'altro.

15.2 Scaricare un'immagine per l'installazione

Per realizzare l'installazione del sistema, la via più semplice è quella di utilizzare una penna USB, un CD o un DVD. Debian ne propone molte varianti, e dunque è necessario iniziare scegliendo il metodo che ci sembra il più adatto alla nostra situazione.

15.2.1 Con o senza driver proprietari?

Alcune periferiche del computer possono aver bisogno, per funzionare, che il sistema sia fornito di un driver non libero. Ma questo non succede sempre.

---

6 Per alcuni componenti, potrebbero esserci dei problemi derivati da difetti di funzionamento nei firmware integrati. Questi problemi a volte vengono corretti tramite degli aggiornamenti forniti dai costruttori stessi. Potrebbe quindi essere una buona idea fare l'aggiornamento del firmware (BIOS o UEFI), dell'Embedded Controller o di altri componenti, prima di procedere con l'installazione. Purtroppo queste procedure sono troppo diverse l'una dall'altra per poterle dettagliare in questa guida, ma generalmente si possono trovare le istruzioni sul sito dei costruttori.

7 Cap. 14

Un dri-cosa?
Questi driver sono dei programmi che hanno la particolarità di poter essere eseguiti su dei chip all'interno della periferica e non all'interno del processore del computer[8]. È il caso per esempio del programma che controlla il movimento delle parti meccaniche di un hard-disk o il funzionamento del sistema radio di una scheda wi-fi. Possiamo benissimo anche non accorgerci della loro esistenza, perché la maggior parte dei driver sono rilasciati direttamente con l'hardware. Ma nel caso di altre periferiche, il sistema operativo deve poter inviare il driver a un componente mentre si avvia.
I driver liberi sono rilasciati con il programma d'installazione di Debian. Purtroppo la maggior parte dei driver non sono liberi[9]. Quindi siamo noi che dobbiamo mettere a disposizione del programma d'installazione di Debian tutti i driver proprietari necessari al funzionamento del computer: questo è il caso tipico di alcune schede wi-fi.

Un'altra storia di compromessi
Se vogliamo installare il nostro sistema cifrato su un computer portatile, è molto probabile che siano necessari dei driver per far andare la scheda wi-fi o per avere una buona risoluzione del monitor.
Su un computer fisso senza wi-fi, è abbastanza plausibile che il nostro sistema cifrato possa funzionare correttamente senza dover aggiungere driver.
Anche se non ne abbiamo prove, potremmo temere che il driver proprietario di una scheda wi-fi possa spiarci a nostra insaputa. D'altra parte, senza quel driver la scheda semplicemente non funzionerà. Ancora una volta si tratta di scendere a compromessi.

8 Cap. 1.2.2
9 Cap. 4.1

15.2.2 L'immagine per l'installazione via rete

Il modo più rapido è quello di utilizzare un'immagine d'installazione via rete, che contiene solo le primissime parti del sistema.
L'installer scaricherà in seguito, tramite internet, il software da installare. È dunque necessario che il computer sul quale vogliamo installare Debian sia connesso a internet, preferibilmente attraverso un cavo di rete (e non con il wi-fi, che all'interno del software d'installazione funziona solo raramente).
Esistono vari file (chiamati "immagini") che contengono una copia dell'immagine d'installazione, a seconda dell'architettura del processore[10]. Nella maggior parte dei casi, occorrerà scaricare quello il cui nome finisce per `amd64-i386-netinst.iso`, detto "multi-architettura", che supporta le architetture a 32 e 64 bit e che funzionerà sulla maggior parte dei computer domestici costruiti dopo il 2006[11].
Poi bisogna scegliere tra la versione contenenti driver proprietari[12] e quella interamente libera, senza software proprietario[13].

15.2.3 L'immagine con l'ambiente grafico

Se non possiamo connettere a Internet il computer sul quale vogliamo installare Debian, possiamo scaricare un DVD contenente tutto il sistema di base, compreso il nostro abituale ambiente grafico. Per fare ciò dobbiamo avere accesso a un masterizzatore DVD o a una penna USB di almeno 4 GB.

---

10 Cap. 1.2.2
11 Alcuni computer portatili utilizzano l'architettura ARM, ma gli autori di questa guida non li hanno mai incontrati per poterli testare...
12 Immagini multi-architettura per l'installazione via rete contenenti i driver proprietari sul sito di Debian [http://cugulo.vado.li/].
13 Immagini DVD per l'installazione di Debian su varie architetture [http://mitapu.vado.li/].

Come per l'installazione via rete, dobbiamo scegliere l'immagine corrispondente alla nostra architettura[14].
Per l'installazione è necessario soltanto il primo DVD. Il nome del file da scaricare può finire con `-i386-DVD-1.iso` (32 bit), o con `-amd64-DVD-1.iso` (64 bit).

15.3 Verificare l'immagine

È buona norma assicurarsi che il download dell'immagine si sia svolto correttamente controllando il checksum dell'installer, per verificarne l'integrità e l'autenticità[15]. Dobbiamo allora procedere in due fasi, nella prima ci assicuriamo dell'integrità, nella seconda dell'autenticità.
Per farlo, è necessario avviare un sistema già installato. Se abbiamo accesso a un computer con GNU/Linux, per esempio quello di un'amica, benissimo. Se disponiamo soltanto di un sistema Live[16], possiamo copiare l'immagine scaricata dentro una penna USB e poi verificarla all'interno del sistema Live.

15.3.1 Verificare l'integrità

Per fare questo dobbiamo seguire la ricetta che riguarda i checksum[17]. Dovremo calcolare il checksum `SHA512` dell'immagine che abbiamo scaricato e verificare se corrisponde a quella contenuto nel file `SHA512SUMS` contenuto nella stessa directory dove abbiamo trovato l'immagine da scaricare.

---

14 Immagini multi-architettura ufficiali per l'installazione via rete sul sito di Debian [http://becozu.vado.li/].

15 Cap. 5

16 Cap. 14

17 Cap. 21

15.3.2 Verificare l'autenticità

Se la verifica dell'integrità è andata bene, dopo aver visto che i due checksum corrispondono, possiamo continuare nel processo verificando l'autenticità. Un avversario avrebbe potuto fornirci un'immagine associata a un checksum, entrambi falsi. La verifica precedente ci permette soltanto di controllare che il file scaricato sia proprio quello che era disponibile sul sito, ma non se sia proprio quello che volevamo ottenere. Dopo aver scaricato il file `SHA1SUMS.sign`, seguire i passi che permettono di verificare la firma crittografica del file `SHA512SUMS`.

15.4 Preparare i supporti per l'installazione

Una volta scelta, scaricata e verificata l'immagine, non ci resta che installarla su una penna USB, un CD o un DVD.

15.4.1 Creare una penna USB per l'installazione

Il caso più facile è quello in cui disponiamo di una penna USB vuota, o che contiene soltanto dati ai quali non teniamo, e in cui abbiamo accesso a un sistema basato su Linux, come Debian o Tails[18].

⚠ *Attenzione*: i dati eventualmente presenti sulla penna andranno perduti. E invece sarà facile analizzare la penna per ritrovare i file il cui contenuto non era stato cancellato "davvero" in precedenza[19]...

- Aprire Volumi, a partire dalla vista d'insieme delle Atti-

18 Cap. 14
19 Cap. 4.3

vità: premere il tasto ⊞ (⌘ su Mac), poi scrivere `volum` e cliccare su “Volumi”.

- Una volta aperta la finestra Volumi, possiamo attaccare la nostra penna USB. Nell’elenco a sinistra apparirà una voce corrispondente. Clicchiamoci per selezionarla.
- Clicchiamo poi sul menu e selezioniamo “Ripristino dell’immagine del volume”. Dentro “Immagine da ripristinare”, selezioniamo l’immagine ISO che abbiamo scaricato. Clicchiamo su “Avviare il ripristino”.
- Ci apparirà un messaggio che ci chiede se vogliamo veramente riscrivere l’immagine sulla periferica. Controlliamo che le dimensioni e il modello della periferica corrispondano alle dimensioni e al modello della nostra penna USB. Se è così, clicchiamo su “Ripristina”.
- A questo punto ci viene chiesta la password di amministrazione, gliela diamo e ci autentichiamo per lanciare la scrittura sulla penna. Una volta finito il ripristino, cliccare su ⏏ per espellere la penna.

15.4.2 Masterizzare l’immagine su un CD o un DVD

Se non abbiamo una penna USB o non abbiamo accesso a un sistema Linux, possiamo masterizzare l’immagine su un CD o un DVD. Il file che abbiamo scaricato è un’“immagine ISO”, ovvero un formato di file che la maggior parte dei programma di masterizzazione riconoscono con questo nome. In generale, se inseriamo un disco vuoto nel lettore, il programma di masterizzazione si occuperà già da solo di trasformare questa immagine scrivendola sul disco – in ogni caso, funziona così su Tails, e in genere anche su Debian e Ubuntu.
Sotto Windows, se non abbiamo già installato un programma capace di masterizzare immagini ISO, il programma libero InfraRecorder farà al caso vostro.

15.5 L'installazione vera e propria

Per installare una Debian cifrata, serve far partire la nostra immagine (che può trovarsi su CD, DVD o penna USB) seguendo la ricetta corrispondente sull'avvio da supporto esterno[20].
Adesso l'installazione vera e propria può iniziare: mettete in conto un po' di tempo e un po' di parole crociate, perché il computer potrebbe dover lavorare per diverso tempo senza che voi dobbiate fare niente di particolare.
Controllate, nel caso di un'immagine d'installazione via rete, che il cavo di rete sia attaccato bene. E se si tratta di un portatile, controllate che sia attaccato bene anche il cavo dell'alimentatore, perché durante l'installazione non vi appariranno le notifiche per la batteria che si sta scaricando.
Il programma di installazione di Debian ha una sua propria documentazione[21]. In caso di dubbi sui passi che stiamo per spiegare, potete darci un'occhiata. Tenete anche presente che per la maggior parte delle scelte che ci verrà chiesto di compiere, il programma di installazione ci proporrà automaticamente una risposta che generalmente funziona...

15.5.1 Avviare l'installer

Facciamo insomma avviare l'immagine (da CD, DVD o penna USB). Ci apparirà un primo menu chiamato "Debian GNU/Linux installer boot menu". Nel caso in cui avessimo scelto un CD multi-architettura, l'opzione selezionata in automatico all'inizio sarà "Graphical install" e troveremo un'altra opzione disponibile "32-bit install options"; in questo caso,

---

20 Cap. 13

21 Il manuale d'installazione è disponibile in diverse versioni. Dovremo seguire quello corrispondente all'architettura del processore. [http://ligenu.vado.li/].

l'installer si è accorto che il nostro processore[22] è compatibile con l'architettura `amd64`, il che comporta qualche vantaggio in termini di sicurezza. Premete invio per proseguire.

15.5.2 Scegliere la lingua e la disposizione della tastiera

- Dopo un po' di pazienza, apparirà un menu chiamato "Select a language": l'installer ci propone di scegliere la lingua dell'installazione. Selezionare l'italiano. Per passare alle tappe successive, bisognerà ogni volta cliccare su "Continua".
- Un altro menu ci chiederà il Paese, per affinare l'adattamento del sistema. Scegliamo il nostro luogo geografico.
- In "Configurare la tastiera", conviene lasciare la scelta di default "IT", salvo esigenze particolari.
- A questo punto l'installer caricherà i file di cui ha bisogno.

15.5.3 Configurazione della rete e "battesimo" della macchina

- L'installer si prende quindi un po' di tempo per configurare la rete. Se il nostro computer ha più di una scheda di rete, bisogna scegliere quella di cui vogliamo servirci durante l'installazione. La scelta di default generalmente è quella giusta, si tratterà di una scheda di rete Ethernet.
- Di seguito ci verrà chiesto il nome della macchina. Scegliamo un nome breve per il nostro computer, tenendo presente che questo nome in seguito risulterà visibile in rete e potrà anche essere scritto nei file creati o modificati.
- L'installer ci chiede poi un "Dominio". Senza entrare

22 Cap. 1.2.2

nei dettagli, è meglio lasciare questo campo vuoto (cancellando quindi quello che l'installer ha eventualmente pre-compilato).

15.5.4 Creare gli utenti e scegliere la password

L'installer ci chiederà adesso di scegliere la password dell'amministratore (*root*). Si tratta di una password necessaria per compiere le operazioni di amministrazione del computer: aggiornamenti, installazione di nuovo software, modifiche importanti al sistema, ecc.
È però più semplice risparmiare un'ulteriore password e permettere che il primo utente creato sul sistema abbia i diritti di compiere le operazioni di amministrazione[23], ridomandandogli la password ogni volta. Per fare questo, basta non inserire alcuna password per l'amministratore: lasciamo quindi semplicemente vuoto il campo e clicchiamo su "Continua".

- In "Nome completo del nuovo utente" scegliamo il nome associato al primo utente creato sul sistema. Questo nome verrà spesso salvato nei documenti creati o modificati; potrebbe quindi essere interessante scegliere un nuovo pseudonimo.
- In "Nome utente", scegliere un nome per il login dell'utente. Viene precompilato, ma potete modificarlo. L'installer fa in modo che, nel caso in cui vogliate cambiarlo, il nome utente cominci con una lettera minuscola seguita da un numero qualsiasi di numeri e lettere minuscole.
- L'installer ci chiede una password per l'utente. Sarà la password con cui si avranno i diritti di amministrare il

23 Questa modalità è chiamata *sudo*, perché dentro il terminale sarà possibile, aggiungendo `sudo` all'inizio della riga, eseguire un comando in qualità di amministratore.

computer, sempre che in precedenza non abbiamo scelto una password per l'utente amministratore.

15.5.5 Partizionare i dischi

A questo punto partirà lo strumento per il partizionamento. Verranno trovate le partizioni presenti e ci verrà proposto di modificarle.

- Nel menu "Metodo di partizionamento", scegliere "Guidato (usa l'intero disco e imposta LVM cifrato)".
- Tra i dischi da partizionare scegliere il disco sul quale vogliamo installare Debian GNU/Linux. Se vogliamo cancellare il sistema attualmente installato, si tratta generalmente del primo disco della lista. Le dimensioni del disco sono un indicatore che permette di non sbagliare, per evitare per esempio di installare Debian sulla penna USB da cui stiamo facendo girare l'installer.
- Ci vengono poi proposti diversi metodi di partizionamento. Scegliamo "Tutti i file in una partizione".
- L'installer ci avverte che stiamo per applicare lo schema di partizionamento che abbiamo scelto, e che ciò sarà irreversibile. Visto che abbiamo prima salvato i dati che volevamo conservare, possiamo rispondere "Sì" alla domanda se vogliamo scrivere le modifiche sui dischi e passare alla configurazione di LVM. A questo punto l'installer procede rimpiazzando il vecchio contenuto del disco con dei dati aleatori. È un'operazione lunga – alcune ore per un disco molto grande – che ci lascia il tempo per fare altre cose.
- Una volta finito, l'installer ci chiederà una passphrase per la cifratura. Scegliamo una buona passphrase[24], digitarla

24 Cap. 12

e poi confermarla riscrivendola una seconda volta.

- L'installer mostrerà l'elenco di tutte le partizioni che sta per creare. Diamogli fiducia e lasciamo che termini il partizionamento e applichi i cambiamenti.
- L'installer ci avvertirà che sta per scrivere le modifiche sul disco. Il disco a questo punto è già stato riempito con dati aleatori, quindi se ci avevamo lasciato sopra dei dati importanti li abbiamo già persi. Possiamo quindi rispondere "Sì" alla domanda se applicare o no i cambiamenti sul disco. Verranno create le partizioni, il che prenderà un po' di tempo.

15.5.6 Installazione del sistema di base

Adesso verrà installato un sistema GNU/Linux minimal. Lasciamolo fare.

15.5.7 Configurare il gestore dei pacchetti

Se l'installer ci propone di utilizzare una fonte diversa da quella che stiamo usando, lasciamo la scelta di default, cioè "No". La domanda seguente riguarda il server dal quale scaricare i programmi. Se non compare in questo momento non dobbiamo preoccuparci, succede solo perché l'installer che stiamo usando non ha bisogno della rete per proseguire. In questo caso, ce lo chiederà più tardi nel corso dell'installazione.

- L'installer ci chiederà di scegliere il paese del mirror dell'archivio Debian. La scelta di default per l'Italia può andare bene se ci troviamo in Italia.
- Ci chiede poi il mirror dell'archivio Debian da utilizzare. La scelta di default "ftp.it.debian.org" va benissimo.

- Ci viene chiesto poi se abbiamo bisogno di un "Proxy HTTP". Lasciamo il campo vuoto.
- A questo punto l'installer proseguirà scaricandosi i file di cui ha bisogno per continuare.

15.5.8 Scelta dei pacchetti

La prossima domanda riguarda il "Concorso Popolarità Pacchetti Debian" e ci chiede se vogliamo partecipare allo studio statistico sull'utilizzo dei pacchetti. Possiamo rispondere di sì senza rischiare di divulgare troppe informazioni supplementari: dato che i programmi verranno in ogni caso scaricati dai server Debian, potrebbero già sapere quali pacchetti stiamo utilizzando, se volessero.
Ora dobbiamo scegliere quali programmi installare. In genere le scelte di base sono: ambiente desktop Debian, server di stampa e Utilità di sistema standard. L'installer si scaricherà tutto il resto del sistema Debian GNU/Linux e l'installerà. È un processo lungo, c'è il tempo di andare a fare qualcos'altro.

15.5.9 Installazione del bootloader GRUB

L'installer propone di impostare il bootloader, il programma che permette di lanciare Linux, su una parte dell'hard-disk chiamata "Master Boot Record (MBR)". Quando ci viene chiesto se installare il bootloader GRUB nel Master Boot Record, rispondiamo di sì.
L'installer chiederà di scegliere la periferica in cui installare il bootloader. Scegliamo l'hard-disk interno, che in genere sarà "/dev/sda". Se abbiamo dubbi, un buon indizio è quello di scegliere il primo disco nella lista il cui nome contenga "ata" o "sata".

Quando avrà finito, l'installer proporrà di riavviare il computer verificando prima che il supporto d'installazione (CD, DVD, penna USB) non sia più inserito al momento del riavvio. Scegliere "Continua".

15.5.10 Avviare il nuovo sistema

Il computer riavvierà il nuovo sistema. A un certo punto ci chiederà la passphrase su una schermata nera: "`Please unlock disk`". Scriviamola, senza preoccuparci del fatto che non si vede cosa stiamo scrivendo, e poi diamo Invio[25].

Dopo l'avvio di un certo numero di programmi, apparirà una schermata con il nome della macchina e il nome dell'utente che abbiamo scelto in precedenza. Selezioniamo l'utente e immettiamo la password associata.

Ecco qua, un nuovo sistema Debian cifrato è pronto per essere utilizzato. Per chi non ne ha mai usato uno può essere una buona idea farsi un giro dentro per familiarizzare con esso. La vista d'insieme delle attività, che si apre cliccando su "Attività" in alto a sinistra o premendo il tasto ⊞ (⌘ su Mac), permette di accedere a molti programmi già installati. Per trovare un programma, si scrive una parola che ne descriva la funzione (per esempio "immagine" per trovare i programmi che lavorano con le immagini). Per visualizzare tutti i programmi installati, clicchiamo in basso a sinistra. Cliccando su "Aiuto", nella vista d'insieme delle attività, possiamo accedere a delle pagine di aiuto contenenti diversi consigli e trucchi.

---

25 Se non abbiamo molta dimestichezza con la tastiera, nei primi tempi potrebbe spesso capitare di fare errori nella frase, per cui non verrà fuori niente. Non preoccupiamoci per i ripetuti errori, insistiamo finché non riusciremo a scriverla giusta. Dopo qualche tempo ci verrà automatico, e gli errori di battitura saranno più rari. Detto ciò, non costa niente verificare sempre di non aver premuto per sbaglio il tasto CapsLock per la maiuscole, altrimenti potrebbe passare molto tempo prima di riuscire a sbloccare l'hard-disk.

15.6 Qualche consiglio per continuare

Potrebbe essere utile a questo punto imparare a fare il backup dei propri dati[26] e a cancellarli davvero[27].
È importante anche imparare a mantenere aggiornato il proprio sistema[28]. Regolarmente vengono scoperti problemi che riguardano i vari programmi, ed è importante installare le correzioni nella misura in cui vengono rese disponibili.

15.7 Un po' di documentazione su Debian e GNU/Linux

Ecco qualche riferimento per la documentazione di Debian e GNU/Linux:

- La guida di riferimento ufficiale di Debian → http://revuza.vado.li/
- La pagina iniziale della documentazione ufficiale per l'utilizzo di Debian → http://zafica.vado.li/
- La guida all'amministrazione di Debian → http://lotusa.vado.li/

Sull'utilizzo di GNU/Linux si trova moltissima documentazione. Queste risorse spesso sono molto utili, ma, come succede sovente su internet, sono purtroppo anche di varia qualità. In particolare, molte di esse smettono di funzionare quando una parte del sistema viene modificato, o terranno poco in considerazione l'intimità che desideriamo preservare nel nostro sistema. Bisogna quindi premunirsi di spirito critico e cercare di capirle bene prima di metterle in pratica.

---

26 Cap. 19
27 Cap. 17
28 Cap. 23

Detto ciò, ecco qualche altra risorsa di wiki e forum:

- Il wiki ufficiale di Debian (tradotto parzialmente dall'inglese) → https://wiki.debian.org/it/FrontPage
- Il forum italiano su Debian → debianitalia.org

16 | Scegliere, verificare e installare un programma

Questa parte propone qualche ricetta riguardo alla gestione dei programmi:

- *Come si trova un pacchetto Debian*?
  Quando vogliamo realizzare nuovi progetti con un computer, spesso dobbiamo installare dei nuovi programmi... ecco qualche consiglio per trovare quel che cerchiamo su Debian[1].
- *Con quali criteri scegliere*?
  A volte dobbiamo scegliere un programma che faccia una determinata cosa e finisce spesso che ci sentiamo spersi nella moltitudine delle soluzioni disponibili. Vediamo quindi qualche criterio che può permetterci di prendere la giusta decisione[2].
- *Come si installa un pacchetto Debian*?
  Una volta che sappiamo quale pacchetto contiene il programma che vogliamo usare, non resta che installarlo correttamente[3].
- *Come si modificano i propri repository Debian*?
  I pacchetti Debian che contengono i programmi si trovano in ciò che viene chiamato *repository*. Anche se quelli forniti da Debian contengono quasi tutti i programmi di cui possiamo aver bisogno, a volte è utile potere aggiungere nuovi repository[4].

1 Cap. 16.1
2 Cap. 16.2
3 Cap. 16.3
4 Cap. 16.4

16.1 Trovare un programma

I software evolvono, per questo è vivamente consigliato utilizzare la versione più aggiornata di questa ricetta, che troverete in francese e in italiano sui siti della Guida https://guide.boum.org/ e https://numerique.noblogs.org/.

Durata: da 5 minuti (se sappiamo il nome del programma che stiamo cercando) a mezz'ora (se partiamo da zero).

Talvolta sappiamo già il nome del programma che vogliamo installare – perché ce l'hanno consigliato, perché l'abbiamo trovato su internet... – e vogliamo sapere se si trova già dentro Debian. Altre volte sappiamo soltanto quello con cui vorremmo il programma ci aiutasse. In ogni caso, il database dei software disponibili dentro Debian risponderà di sicuro alla nostra domanda.
Per compiere delle scelte oculate, dato che ci sono vari programmi che fanno la stessa cosa, potete consultare la ricetta "Scegliere un programma" nelle pagine seguenti[5].

- Aprire il "Gestore dei pacchetti": accedere alla vista d'insieme delle Attività premendo il tasto ⊞ (⌘ su Mac), poi scrivere `pacchett` e cliccare su "Gestore dei pacchetti Synaptic".
- Dato che il gestore dei pacchetti consente di modificare i programmi installati nel computer, e dunque di scegliere di quali programmi fidarsi, ci sentiremo rassicurati dal fatto che per aprirlo ci verrà chiesta la nostra password.
- Una volta dentro il gestore dei pacchetti, iniziamo aggiornando la lista dei pacchetti disponibili cliccando sull'icona "Aggiorna". Il gestore di pacchetti si scaricherà da un

5 Cap. 16.2

server Debian le ultime informazioni sui pacchetti disponibili.

- Ci sono due tecniche per cercare un pacchetto:
  a) cliccare sull'icona "Cerca" nella barra degli strumenti. Qui verificare che in "Cerca in" sia selezionato "Descrizione e nome". Scrivere delle parole chiave o il nome dell'applicazione nel campo "Cerca" (per esempio "dizionario tedesco openoffice"). Le descrizioni dei programmi poco usati raramente sono tradotti dall'inglese, provate quindi anche in inglese. Cliccare su "Cerca" per lanciare la ricerca;
  b) selezionare una categoria nella colonna di sinistra.
- I risultati della ricerca o i pacchetti della categoria saranno visualizzati nella lista in alto a destra. Cliccando sul nome di un pacchetto, apparirà la sua descrizione nel riquadro in basso a destra.
- Non resta adesso che installare il pacchetto corrispondente (vedi pagine seguenti[6]).

16.2 Criteri di scelta

I software evolvono, per questo è vivamente consigliato utilizzare la versione più aggiornata di questa ricetta, che troverete in francese e in italiano sui siti della Guida https://guide.boum.org/ e https://numerique.noblogs.org/.

Durata: da una mezz'ora a un'ora.

Abbiamo già spiegato i motivi per cui scegliere dei software liberi invece che proprietari[7]. Nelle pagine seguenti vedremo quindi solo quali scegliere tra questi.

6 Cap. 16.3
7 Cap. 4.1

16.2.1 Metodi di installazione

In genere è meglio installare il software fornito dalla propria distribuzione GNU/Linux (ad esempio Debian). Per due fondamentali motivi.
Prima di tutto per una questione pratica: la distribuzione fornisce gli strumenti per installare e aggiornare, in modo più o meno automatico, un insieme di programmi; in questo modo veniamo anche messi in guardia quando viene trovata una falla di sicurezza in uno dei programmi che stiamo utilizzando. Quando invece installiamo un software che non è fornito con la nostra distribuzione, siamo lasciati a noi stessi: dobbiamo ricordarci noi di aggiornarlo, tenerci informati sugli eventuali buchi di sicurezza che possono venire scoperti, gestire le dipendenze tra programmi. Questo comporta energie, tempo e competenze.
Poi c'è anche una questione di sicurezza: quando si sceglie una distribuzione GNU/Linux si decide implicitamente di fidarci di una comunità, di un processo di produzione. Installare un software che non è fornito con quella distribuzione vuol dire prendere di nuovo una simile decisione riguardo a un'altra comunità e a un altro processo di produzione. Questa decisione non va presa alla leggera: quando si decide di installare un programma che non appartiene alla nostra distribuzione, stiamo allargando l'insieme di persone e di procedure di cui ci stiamo fidando, aumentando quindi i rischi.

16.2.2 Maturità

L'attrazione verso il nuovo, spesso è una trappola.
Quando è possibile, sarebbe invece meglio scegliere un programma che abbia raggiunto una certa maturità: è probabile che all'interno di un software sviluppato attivamente e utiliz-

zato almeno da qualche anno, i principali problemi siano già stati scoperti e corretti… compresi i buchi di sicurezza.
Per rendersene conto basta consultare lo storico di ciascun programma, sul rispettivo sito web o dentro un file chiamato `Changelog`, generalmente distribuito insieme al software.

16.2.3 Processo di produzione e comunità

La dicitura software libero è un criterio essenzialmente giuridico, che non deve mai bastare per ispirarci fiducia[8].
Certo, il fatto che un software venga rilasciato sotto una licenza libera, apre la possibilità a un tipo di sviluppo rassicurante. Ma le persone che sviluppano questo software potrebbero benissimo, intenzionalmente o no, scoraggiare ogni tipo di cooperazione e lavorare in modo isolato. Cosa importa allora che il programma sia *giuridicamente* libero se, di fatto, nessun altro potrà mai leggerne il codice?
Bisogna quindi studiarsi rapidamente il processo di produzione dei software che stiamo prendendo in esame, aiutandosi con le domande qui sotto, che ci permetteranno inoltre di giudicarne il dinamismo:

- Chi è che lo sviluppa? Una persona, più persone, un intero gruppo?
- Il numero di persone che contribuisce al codice sta aumentando o diminuendo?
- Lo sviluppo è attivo? In questo caso non si tratta di velocità, ma di reattività, di mantenimento nel lungo termine, di resistenza. Lo sviluppo di un software è una maratona, non uno sprint.

8 Cap. 4.1.3

E riguardo gli strumenti di comunicazione collettiva sui quali si appoggia lo sviluppo (mailing-list e forum di discussione, per esempio):

- Si può accedere con facilità alle discussioni che riguardano lo sviluppo del codice?
- Queste discussioni coinvolgono molte persone?
- Sono solo gli utenti a partecipare a queste discussioni?
- Che atmosfera c'è? Calma piatta, silenzio tombale, una gioiosa cacofonia, serietà glaciale, braccia aperte, implicita ostilità, tenera complicità...?
- Il volume delle discussioni, negli ultimi anni/mesi, sta diminuendo o aumentando? Più che il rumore di fondo, ciò che importa sono soprattutto i messaggi che ottengono una risposta: un software maturo, stabile e ben documentato non sarà necessariamente fonte di discussione, ma se non c'è nessuno pronto a rispondere alle domande dei neofiti, questo potrebbe essere un brutto segno.
- Si trovano dei feedback, dei suggerimenti di miglioramento? Se sì, vengono presi in considerazione?
- Le risposte vengono date sempre da un numero ridotto di persone, oppure esistono delle pratiche più larghe di mutuo aiuto?

16.2.4 Popolarità

La popolarità è un criterio delicato in materia di software. Il fatto che la maggior parte dei computer negli uffici funzionino attualmente con Windows non significa affatto che Windows sia il miglior sistema operativo a disposizione.
Ma d'altra parte, se un software non è utilizzato da nessuno viene da mettere in dubbio la sua sopravvivenza nel lungo periodo: se il team di sviluppo smettesse di lavorare su questo

software, cosa ne sarebbe? Chi se ne farebbe carico?
Come regola generale, dobbiamo quindi scegliere un software usato da un numero sufficientemente importante di persone, ma non per forza il più utilizzato.
Per misurare la popolarità di un programma, è possibile da un lato utilizzare gli stessi criteri che abbiamo descritto sopra riguardo il dinamismo della comunità che ha intorno. Dall'altro, Debian pubblica i risultati del suo "popularity contest"[9], che permette di confrontare non solo il numero di persone che hanno installato questo o quel programma, ma anche e soprattutto l'evoluzione nel tempo della loro popolarità.

16.2.5 Lo storico sulla sicurezza

Ecco un altro criterio a doppio taglio. Si può cominciare dando un'occhiata agli avvisi di sicurezza[10] proposti da Debian. Cercando un programma con il suo nome, si ottiene la lista dei problemi di sicurezza che sono stati scoperti e, a volte, risolti.
Se un programma ha uno storico sulla sicurezza perfettamente immacolato, potrebbe implicitamente voler dire o che tutti se ne fregano, o che il codice è stato scritto in modo estremamente rigoroso.
Se invece sono stati trovati dei buchi di sicurezza, ci possono essere diverse implicazioni, a volte contradditorie tra loro.

1. I buchi sono stati scoperti e corretti:
   - quindi non esistono più, a priori;
   - quindi qualcuno si è preoccupato di trovarli e qualcun altro di correggerli: si suppone un'attenzione alla questione.

9 https://popcon.debian.org
10 Il Security Team di Debian mantiene le informazioni riguardo ciascun pacchetto nel *Security Tracker*. https://security-tracker.debian.org

2. Questi buchi esistevano:
    - il codice potrebbe essere stato scritto senza una cura particolare alla sicurezza;
    - potrebbero esisterne altri, non ancora scoperti o, peggio, non ancora resi pubblici.

Per affinare il nostro intuito rispetto a un software, potrebbe essere utile fare affidamento sul criterio del "tempo": per esempio, non è una cosa drammatica se all'inizio dello sviluppo di un software vengono scoperti dei buchi e poi non ne sono stati scoperti altri per un po' di anni; potremmo considerarli errori di giovinezza. Al contrario, se vengono regolarmente scoperte nuove falle, da anni e anche recentemente, è ragionevole pensare che il software abbia ancora molti problemi di sicurezza totalmente sconosciuti... o non resi pubblici. Ma un numero relativamente alto di problemi, anche recenti, può indicare una comunità di sviluppo attiva ed è un segno migliore rispetto a nessuna falla, perché in quel caso vorrebbe dire che nessuno se ne occupa.

16.2.6 Team di sviluppo

Chi ha scritto questo software? Se siamo in grado di rispondere a questa domanda, ci sono diversi fattori che possono aiutarci a determinare che grado di fiducia accordare al team di sviluppo. Per esempio:

- Le stesse persone hanno scritto anche un altro software, che stiamo già usando frequentemente; le nostre impressioni su quest'altro software sono molto utili per farci un'idea.
- Certi membri del team di sviluppo hanno dei indirizzi mail che finiscono per `@debian.org`, e hanno quindi il per-

messo di modificare i programmi forniti da Debian GNU/Linux; se stiamo usando questa distribuzione, stiamo già fidandoci, in qualche modo, di queste persone.

- Altri membri del team di sviluppo hanno degli indirizzi mail che finiscono per `@google.com`, e questo indica che li paga Google; anche se non vi è alcun dubbio sulle loro competenze tecniche, possiamo chiederci fino a che punto il loro lavoro venga manovrato dai loro datori di lavoro che, invece, non meritano nessuna fiducia riguardo alla salvaguardia dei vostri dati personali.

16.3 Installare un pacchetto Debian

I software evolvono, per questo è vivamente consigliato utilizzare la versione più aggiornata di questa ricetta, che troverete in francese e in italiano sui siti della Guida https://guide.boum.org/ e https://numerique.noblogs.org/.

Durata: 5 minuti, più il tempo di scaricamento e installazione (da qualche secondo ad alcune ore, a seconda della grandezza del software da installare e dalla velocità della connessione).

16.3.1 Aprire il gestore dei pacchetti

Una volta che sappiamo in quale pacchetto è contenuto il programma che vogliamo utilizzare, non resta che installarlo.
Per farlo utilizzeremo il gestore dei pacchetti Synaptic, che possiamo aprire partendo dalla vista d'insieme delle attività e premendo il tasto ⊞ (⌘ su Mac), poi scrivendo "pacchetto" e cliccando su "Gestore dei pacchetti Synaptic".

Dato che il gestore dei pacchetti consente di modificare i programmi installati sul computer, per aprirlo viene richiesta una password.

16.3.2 Aggiornare la lista dei pacchetti disponibili

Una volta dentro al gestore dei pacchetti, iniziamo aggiornando la lista dei pacchetti disponibili cliccando sull'icona "Aggiorna". Il gestore dei pacchetti scaricherà dai server Debian le ultime informazioni sui pacchetti disponibili.

16.3.3 Cercare il pacchetto da installare

A questo punto va trovato il pacchetto che vogliamo installare. Clicchiamo sull'icona "Cerca" nella barra degli strumenti. Qui, se conosciamo il nome di questo pacchetto, lo scriveremo nel campo "Cerca", dopo aver selezionato "Nome" nel menu a tendina "Cerca in".

16.3.4 Selezionare il pacchetto da installare

Adesso arriva la fase vera e propria d'installazione del pacchetto che abbiamo precedentemente trovato. Ci sono diversi modi per farlo, a seconda che si preferisca utilizzare la versione disponibile nei repository ufficiali oppure un pacchetto proveniente da un altro repository, per averne ad esempio una versione più recente.

Installare la versione predefinita
Normalmente il pacchetto cercato si trova da qualche parte all'interno della lista dei pacchetti. Una volta trovata la riga

corrispondente, ci clicchiamo sopra con il tasto destro e nel menu che appare scegliamo “Installa”.
Se questo pacchetto dipende da altri pacchetti, il gestore dei pacchetti aprirà una finestra dove ci chiederà di “Selezionare le ulteriori modifiche richieste”. In genere le sue proposte sono sensate, possiamo quindi accettare cliccando su “Aggiungi alla selezione”.

Installare una versione particolare
A volte capita di dover installare una versione particolare di un pacchetto. Per esempio nel caso in cui siano stati aggiunti dei repository specifici[11]. Invece di scegliere “Installa” nel menu contestuale, selezioniamo il pacchetto desiderato cliccando col tasto sinistro, senza cliccare sulla casella accanto, e poi nel menu “Pacchetto” scegliere “Forza versione...”. Selezioniamo quindi la versione desiderata. Il resto non cambia rispetto alla procedura per installare una versione predefinita.

16.3.5 Applicare le modifiche

Possiamo ripetere gli ultimi due passaggi per installare più pacchetti allo stesso tempo. Una volta che abbiamo preparato l’installazione, non resta che lanciarla cliccando su “Applica” nella barra degli strumenti. Il Gestore dei pacchetti aprirà una finestra “Riepilogo”, dove verranno elencate tutte le operazioni che stanno per essere compiute. Dopo averci dato un’occhiata per controllare che non ci siano errori, clicchiamo su “Applica”.
Il gestore scaricherà i pacchetti da internet, li verificherà e poi li installerà. Potrebbe capitare che il Gestore avverta che alcuni pacchetti non hanno potuto essere verificati: questa in-

---

11 Cap. 16.4

formazione non è da prendere alla leggera. In questo caso è meglio annullare lo scaricamento, clicchiamo su "Aggiorna", nel menu principale, e ricominciamo l'operazione della selezione dei pacchetti. Se il messaggio appare un'altra volta, si potrebbe trattare di un attacco, di una svista tecnica o di un semplice errore di configurazione. In ogni caso è meglio rinunciare a installare nuovi pacchetti finché non abbiamo capito la fonte del problema.
Infine, se tutto è andato bene, il gestore di pacchetti mostrerà una finestra in cui dice che le modifiche sono state applicate. A questo punto è buona regola chiudere il Gestore dei pacchetti per evitare che possa cadere in altre mani.

16.4 Utilizzare dei backport

I software evolvono, per questo è vivamente consigliato utilizzare la versione più aggiornata di questa ricetta, che troverete in francese e in italiano sui siti della Guida https://guide.boum.org/ e https://numerique.noblogs.org/.

Durata: da un quarto d'ora a una mezz'ora.

I pacchetti Debian che contengono i programmi si trovano dentro quello che viene chiamato un repository. Se i repository forniti con Debian contengono quasi tutti i programmi di cui potremmo aver bisogno, a volte è invece utile installare dei programmi più recenti rispetto a quelli contenuti nell'ultima versione stabile di Debian. Questi pacchetti vengono chiamati backport.

Attenzione: Aggiungere un nuovo repository Debian su un computer significa fidarsi delle persone che se ne occupano. Anche se i repository backport di cui parliamo qui di seguito

sono mantenuti da membri di Debian, per molti altri repository non è così. La decisione di fidarsi di loro non deve essere presa alla leggera: se il repository in questione contiene del software malevolo[12], ce lo ritroveremo installato sul computer senza neanche rendercene conto.

16.4.1 Aprire il gestore dei pacchetti

Aprire il Gestore dei pacchetti: accedere alla vista d'insieme delle attività premendo il tasto ⊞ (⌘ su Mac), poi scrivere `pacchett` e cliccare su "Gestore dei pacchetti Synaptic".
Dato che il gestore dei pacchetti consente di modificare i programmi installati nel computer, e dunque di scegliere di quali programmi fidarsi, ci sentiremo rassicurati dal fatto che per aprirlo ci verrà chiesta la nostra password.

16.4.2 Configurare i repository

Cliccare sulla voce "Repository" nel menu "Impostazioni" e poi cliccare sul menu "New". Nella riga che inizia per "URI" scrivere l'indirizzo APT aggiungendo:

```
deb http://ftp.it.debian.org/debian/ stretch-backports
main
```

In questo caso, la versione del repository è *stretch-backports* e la categoria è main. Se volessimo installare anche del software non libero possiamo aggiungere anche `contrib` e `non-free` alla fine dell'indirizzo:

12 Cap. 3.2

```
deb http://ftp.it.debian.org/debian/ stretch-backports
main contrib non-free
```

Una volta fatto questo, clicchiamo su “OK”.

16.4.3 Aggiornare i pacchetti disponibili

A questo punto clicchiamo su “Esci”, nel menu “File”. Probabilmente si aprirà una finestra “Repository modificati”, nel qual caso basterà cliccare su “Aggiorna”. Se non succedesse, bisogna cliccare su “Aggiorna” per aggiornare la lista dei pacchetti.
Nell’estate del 2017, un bug ha fatto sì che venisse fuori una finestra con un messaggio d’errore di questo tipo:

```
W: http://ftp.it.debian.org/debian/dists/stretch-
backports/
InRelease: The key(s) in the keyring /etc/apt/tru-
sted.gpg are ignored as the file in not readable by
user ‘_apt’ executing apt-key
```

Non si tratta di un errore bloccante, ma di un avvertimento. Basta cliccare sul bottone “Chiudi” e ignorarlo.

17 | Cancellare dei dati "per davvero"

Negli scorsi capitoli abbiamo visto che quando cancelliamo un file, il suo contenuto non viene davvero eliminato[1]. Nonostante ciò, esistono dei programmi che permettono di cancellare dei file e il loro contenuto, o almeno che ci provano, con tutti i limiti che spiegheremo più avanti.

17.1 Un po' di teoria

17.1.1 Il metodo Gutmann

La documentazione[2] del pacchetto *secure-delete* che utilizzeremo nella ricetta seguente, ispirata da una pubblicazione di Peter Gutmann pubblicata nel 1996[3], dice:

Il processo di cancellazione funziona in questo modo:

1. *la procedura di distruzione (in modo sicuro) rimpiazza il contenuto di un file 38 volte. Dopo ciascun passaggio, la cache del disco viene ripulita;*
2. *il file viene smembrato, in modo che un attaccante non sappia quali blocchi del disco appartengano al file;*
3. *il file viene rinominato, in modo che un attaccante non possa trarre conclusioni sul contenuto del file soppresso a partire dal suo nome;*
4. *alla fine di tutto ciò, il file viene cancellato. [...]*

---

1 Cap. 4.3

2 Il file `README.gz` dentro `/usr/share/doc/secure-delete` all'interno di una distribuzione Debian.

3 Peter Gutmann, 1996, *Secure Delection of Data from Magnetic and Solid-State Memory* [http://gebeve.vado.li/].

17.1.2 Il compromesso adottato

Lo studio di Peter Gutmann si basava su delle tecnologie di hard-disk che al giorno d'oggi non esistono più. Alla fine del suo articolo, un paragrafo intitolato *Epilogo* in sostanza diceva che per un hard-disk "recente"[4], le 38 scritture successive non sono più necessarie: basta sovrascrivere più volte i dati con degli altri dati aleatori. Ma, a parte la natura e il numero delle riscritture, il processo che aveva descritto resta perfettamente attuale anche per gli hard-disk odierni. Questo metodo non è però adatto per i dischi SSD[5]. E dal momento che i dischi SSD attualmente stanno tendendo a rimpiazzare gli hard disk...
Inoltre, il NIST (*National Institute of Standards and Techonology*, organismo governativo degli Stati Uniti che definisce i protocolli di sicurezza utilizzati, tra gli altri, dalle amministrazioni di quel Paese) ha pubblicato di recente uno studio[6] della NSA, che sembra concludere che sugli hard-disk moderni, i dati sono talmente appiccicati l'uno con l'altro che diventa praticamente impossibile affidarsi a delle analisi magnetiche per recuperare le tracce dei dati cancellati; in effetti, la densità dei dati degli hard-disk è in continua crescita, per permettere di aumentare la capacità di stoccaggio.
Di conseguenza, nelle ricette seguenti ci accontenteremo di qualche passaggio aleatorio, rifacendoci alla messa in pratica del metodo originale di Gutmann.
Si tratta ancora una volta di trovare caso per caso un compromesso tra rapidità e livello di protezione desiderato[7], a seconda della grandezza dei dati da cancellare, dell'età dell'hard-disk e di quanto ci fidiamo del NIST.

---

4 Che utilizza la tecnologia PRML [http://matiga.vado.li/], comparsa nel 1990 [http://gavide.vado.li/].

5 Cap. 4.3.3

6 NIST, 2006, *Guidelines for Media Sanitization* [http://fetego.vado.li/].

7 Cap. 7

17.1.3 Penne USB, dischi SSD e altre memorie flash

Riguardo alle penne USB o altre memorie flash – come le schede SD, o i dischi SSH – uno studio del 2011[8] ha mostrato che la situazione è davvero problematica.
Questo studio dimostra che è impossibile, a prescindere dal numero di riscritture, avere la garanzia che tutto il contenuto di un file sia stato completamente sovrascritto. Anche se rendessimo inaccessibili i dati semplicemente togliendo la penna, essi sarebbero lo stesso visibili da chiunque guardasse direttamente dentro i chip della memoria flash.
Il solo metodo che ha funzionato in modo sistematico, è stato quello di riscrivere più volte completamente la penna USB. Nella maggior parte dei casi, due passaggi sono sufficienti, ma per alcuni modelli sono state necessarie venti riscritture prima che i dati scomparissero per davvero.
Dati questi presupposti, la soluzione preventiva pare essere quella di cifrare sistematicamente le penne USB[9], operazione che rende ben più difficile l'estrazione delle informazioni direttamente dai chip della memoria flash. E per ripulirle a posteriori, la formattazione per intero malgrado i suoi limiti, protegge almeno dagli attacchi via software.

17.1.4 Altri limiti della cancellazione "sicura"

Sopratutto se si utilizza un file system journaled come ext3, ext4, ecc., oppure un sistema di scrittura, di compressione o di backup, sull'hard-disk (come RAID) o via rete, possono ancora rimanere delle informazioni sui file che permettono di recuperarli. Ne abbiamo parlato al capitolo 4.3.

---

8 Michael Wei et Al, 2011, *Reliably Erasing Data From Flash-Based Solid State* [http://dozesa.vado.li/].
9 Cap. 18

17.2 Riguardo agli altri sistemi

Abbiamo visto che se utilizziamo un sistema operativo proprietario, è un'illusione pensare di poter raggiungere una vera intimità[10]. Anche se esistono dei programmi che dovrebbero eliminare i file e il loro contenuto sotto Windows e Mac OS X, è difficile pensare di poterci fare affidamento.

17.3 Iniziamo

Ciò che è possibile cancellare:

- i file singoli;
- un'intera periferica;
- dei file già cancellati.

17.4 Eliminare dei file... e il loro contenuto

I software evolvono, per questo è vivamente consigliato utilizzare la versione più aggiornata di questa ricetta, che troverete in francese e in italiano sui siti della Guida https://guide.boum.org/ e https://numerique.noblogs.org/

Durata: 5 minuti di preparazione, più da qualche secondo a qualche ora d'attesa in base alla grandezza dei file da cancellare e del metodo usato.

Ecco quindi il metodo da seguire per sbarazzarsi dei file in modo tale da rendere illeggibile il loro contenuto.

---

10 Cap. 4

⚠ *Attenzione*: Questo metodo funziona unicamente con gli hard-disk meccanici. Se sovrascrivete il contenuto di un file all'interno di una penna USB (o su un altro supporto che utilizza la memoria flash come ad esempio una scheda SD o un disco SSD) ci sono buone possibilità che il file risulti ancora leggibile in una zona inaccessibile della periferica!

17.4.1 Installare i programmi necessari

Se non l'abbiamo già fatto, bisogna installare[11] `nautilus-wipe` e poi riavviare il computer.
Questo pacchetto è presente di default in Tails.

17.4.2 Eliminare dei file e il loro contenuto a partire dal file manager

In Tails
Per eliminare dei file e il loro contenuto utilizzando Tails, consultiamo la documentazione cliccando sull'icona "Documentazione di Tails" che si trova sul Desktop.
Cliccare su "Documentazione", nel menu a destra. Dentro l'indice, cercare la sezione "Cifratura e vita privata" e cliccare sulla pagina "Cancellare dei file in modo sicuro e ripulire lo spazio disco con Nautilus Wipe".

In una Debian cifrata
Per cancellare dei file e il loro contenuto a partire dal file manager, risaliamo al file, clicchiamoci sopra con il tasto destro del mouse e selezioniamo "Elimina". Si aprirà una finestra che ci chiederà di confermare l'eliminazione, proponendoci anche

11 Cap. 16.3

alcune opzioni. Possiamo scegliere il numero di passaggi da effettuare per sovrascrivere i dati della nostra periferica e anche alcune opzioni di comportamento circa l'eliminazione dei dati. Le opzioni di default sono più che sufficienti per gli attuali hard-disk.
Clicchiamo ora su "Cancella". Una volta che la cancellazione è terminata si aprirà una finestra "Cancellazione riuscita" per dare conferma che gli elementi siano stati eliminati.

17.5 Cancellare "per davvero" un intero disco

Prima di disfarsi di un hard-disk, di riciclarlo, di installare un nuovo sistema operativo[12] o anche solo di mandare un computer rotto all'assistenza, può essere saggio provare a mettere dei bastoni tra le ruote di chi volesse recuperare i dati che esso conteneva. Per farlo, la migliore soluzione è sempre quella di sovrascrivere tutto con cose a caso.
Prima di utilizzare questa ricetta, bisogna pensarci bene e farsi un attento backup dei dati che vogliamo conservare[13]. Se applicheremo bene questa ricetta, essa renderà effettivamente i file molto difficili da recuperare, anche analizzando il disco in laboratorio.
Vediamo prima di tutto come cancellare tutto il contenuto di un disco, poi come rendere rapidamente inaccessibile il contenuto di una partizione cifrata.

17.6 Cancellare l'intero contenuto di un disco

↻ I software evolvono, per questo è vivamente consigliato utilizzare la versione più aggiornata di questa ricetta, che tro-

12 Cap. 8
13 Cap. 19

verete in francese e in italiano sui siti della Guida https://guide.boum.org/ e https://numerique.noblogs.org/

Durata: 5 minuti di preparazione, poi alcune ore di attesa a seconda della grandezza del disco.

Per cancellare un intero volume (disco o partizione), utilizzeremo il comando `shred` in modo da fargli sovrascrivere per tre volte con dei contenuti aleatori la totalità dei dati. Questo comando permette quindi, oltre alla cancellazione dei file, di sovrascrivere lo spazio cancellato in modo che diventi quasi impossibile ritrovare cosa contenesse in precedenza.
Per sovrascrivere il contenuto di un disco, non dobbiamo stare attualmente utilizzando quello stesso disco... Se contiene il sistema operativo che usiamo abitualmente, bisogna quindi mettere l'hard-disk dentro un altro computer oppure utilizzare un sistema Live[14]. `shred` è uno strumento base standard, indipendentemente da quale Live utilizzeremo.
Il comando è molto semplice. Ha bisogno soltanto di sapere la locazione della periferica (il suo percorso) che vogliamo eliminare, e poi di un po' di pazienza, perché il processo prenderà diverse ore.

17.6.1 Trovare il percorso di una periferica

Prima di tutto bisogna saper individuare, senza errori, il percorso utilizzato dal sistema operativo per localizzare la periferica che vogliamo cancellare.
Se dobbiamo cancellare un disco interno, cominciamo smontando tutti gli hard-disk esterni, penne USB, lettori di schede o altre periferiche attaccate al computer. Da una parte questo

14 Cap. 14

ci eviterà di cancellarle per errore, dall'altra renderà la ricerca del nostro hard-disk più facile.
Ovviamente non dobbiamo fare niente di tutto ciò se è proprio il contenuto di un disco esterno quello che vogliamo rendere inaccessibile.

Aprire l'utility del disco
Apriamo "Dischi": accediamo alla vista d'insieme delle Attività cliccando sul tasto ⊞ (⌘ su Mac), poi scrivere `disc` e cliccare su "Dischi".

Cercare l'indirizzo di una periferica
La colonna di sinistra mostra l'elenco dei dischi del sistema conosciuti. Possiamo cliccare su uno di questi e vedremo apparire a destra più informazioni. L'icona, la grandezza e il nome stesso, dovrebbero consentirci di identificare quello che cerchiamo.
Se questo non dovesse bastare, possiamo dare un'occhiata all'organizzazione delle partizioni, guardando la tabella che appare nella parte di destra:

- se il disco da cancellare contiene un sistema GNU/Linux non cifrato, ci devono essere almeno due partizioni, una con un file system *swap*, l'altra generalmente con *ext3* o *ext4*;
- se il disco da cancellare contiene un sistema GNU/Linux cifrato, devono esserci almeno due partizioni, una con un file system *ext2* e l'altra *LUKS*;
- se il disco da cancellare contiene un sistema Windows, dovrebbero esserci una o più partizioni chiamate *ntfs* o *fat32*.

In genere, la periferica che corrisponde al disco interno è la prima della lista.

Una volta trovato e selezionato il disco, potremmo leggerne l'indirizzo nella parte in basso a destra, accanto al titolo "Periferica".
L'indirizzo della periferica inizia per `/dev/` seguito da tre lettere e una cifra, i primi caratteri nella maggior parte dei casi saranno `sd`, `hd` o `mmcblk`: per esempio `/dev/sdx1`. Segnatevi l'indirizzo da qualche parte, senza la cifra finale (per esempio `/dev/sdx`): d'ora in poi dovremo scrivere quello al posto di `LA_PERIFERICA`.

⚠ *Attenzione*: Questo indirizzo non è necessariamente sempre lo stesso. Sarà meglio riprovare questa piccola procedura dopo aver riavviato il computer, attaccato e staccato una penna USB o un hard-disk. Questo ci eviterà brutte sorprese… come quella di perdere il contenuto dell'hard-disk sbagliato.

17.6.2 Lanciare il comando `shred`

Apriamo un terminale[15]: apriamo la vista d'insieme delle attività cliccando sul tasto ⊞ (⌘ su Mac), poi scrivere `term` e cliccare su "terminale".
Scrivere il comando seguente sostituendo `LA_PERIFERICA` con l'indirizzo della periferica che abbiamo trovato prima:

```
pkexec shred -n 3 -v LA_PERIFERICA
```

Se preferiamo utilizzare il metodo originale di Gutmann (più lungo, e forse più sicuro), dobbiamo sostituire `-n 3` con `-n 25`. Una volta scritto e controllato il comando, premere Invio. Ci verrà chiesta una password, perché questo comando necessita dei privilegi di amministrazione[16]. A questo punto il coman-

15 Cap. 11
16 Cap. 11

do `shred` scriverà sul terminale quello che sta facendo (perché gliel'abbiamo chiesto noi, aggiungendo al comando `shred` l'opzione `-v` che in questo caso significa che il computer dovrà essere "verboso" cioè "chiacchierone"):

```
shred: /dev/sdb: pass 1/3 (random)…
shred: /dev/sdb: pass 2/3 (random)…
shred: /dev/sdb: pass 3/3 (random)…
```

Alla fine di questa procedura, il terminale restituirà di nuovo il segno `$`, che indica il prompt. A questo punto possiamo chiudere il terminale.

17.6.3 Riutilizzare il disco

Attenzione, questo metodo non soltanto cancella i dati di un intero volume ma, alla fine dell'operazione, il disco non avrà più una tabella di partizioni[17], né un file system. Per poterlo riutilizzare, è necessario creare da capo almeno una nuova partizione e il suo file system[18], attraverso l'utility Dischi, per esempio.

17.7 Rendere irrecuperabili dei dati già cancellati

↻ I software evolvono, per questo è vivamente consigliato utilizzare la versione più aggiornata di questa ricetta, che troverete in francese e in italiano sui siti della Guida https://guide.boum.org/ e https://numerique.noblogs.org/

17 Cap. 1.5.1
18 Cap. 1.5.2

Durata: 5 minuti di preparazione, più da qualche minuto a qualche ora d'attesa, a seconda della dimensione del disco da ripulire e a seconda del metodo usato.

Se i file sono già stati cancellati senza precauzioni particolari, i dati che contenevano si trovano ancora sul disco. L'obiettivo di questa ricetta è quello di sovrascrivere quei dati superstiti, ripulendo lo spazio libero di un hard-disk. Questo metodo quindi non cancella nessun file visibile nel gestore dei file.

Attenzione: Come gli altri metodi di cancellazione di un file "per davvero", questo metodo non funziona con alcuni tipi di file system "intelligenti" che, per essere più efficaci, non mostrano tutto lo spazio libero al programma incaricato di coprire le tracce. Come abbiamo detto all'inizio del capitolo, non si deve fare affidamento su questo metodo per una penna USB, delle schede SD o dei dischi SSD per i quali è invece preferibile sovrascrivere più volte l'intero disco.

In Tails
Il pacchetto `nautilus-wipe` è installato di default dentro Tails. Ci basta quindi consultare la documentazione cliccando sull'icona "Documentazione di Tails" sulla Scrivania.
Nel menu a destra, clicchiamo su "Documentazione". Poi, all'interno dell'indice che si aprirà, cerchiamo la sezione "Cifratura e vita privata" e clicchiamo sulla pagina "Cancellare dei file in modo sicuro e ripulire lo spazio disco con Nautilus Wipe".

Con una Debian cifrata
Se non l'abbiamo ancora fatto, installiamo il pacchetto `nautilus-wipe` e poi riavviamo il computer.
A questo punto apriamo il gestore dei file e risaliamo al disco che vogliamo ripulire. Clicchiamo col tasto destro nella parte

destra del gestore dei file e selezioniamo “Cancellare lo spazio disco disponibile”. Si aprirà una finestra che ci chiederà di confermare la cancellazione dello spazio disco disponibile e ci proporrà anche qualche opzione.
Possiamo scegliere il numero di passaggi effettuati per sovrascrivere i dati della nostra periferica e anche qualche opzione che riguarda il comportamento durante la cancellazione. Le opzioni di default sono sufficienti per gli hard-disk attuali.
Adesso clicchiamo su “Cancellare lo spazio disco disponibile”. La cancellazione può impiegare diverso tempo. In alcuni casi ci verrà chiesta la password di amministrazione.
Vedremo che è stata creata una cartella chiamata “tmp. XXXXXXXXXXXX” all’interno della cartella. Nautilus Wipe ci crea un file all’interno, aumentandone la grandezza fino al massimo della disponibilità, in modo da utilizzare tutto lo spazio libero disponibile e poi lo cancellerà in modo sicuro. Una volta finita la cancellazione, spunterà una finestra “La cancellazione è riuscita”, precisando che “Lo spazio disco disponibile sulla partizione o sulla periferica [...] è stato ripulito con successo”.

18 | Partizionare e cifrare un hard-disk

Impariamo adesso a cifrare un dispositivo, per poterci salvare dentro i dati in modo cifrato.
Una volta cifrato il disco, i dati che esso contiene sono accessibili soltanto previo inserimento di una password che permette di decifrarlo. Per avere ulteriori informazioni, consultate la parte sulla crittografia[1].
Quando si conosce la password si ha accesso ai dati dell'hard-disk in questione, è bene quindi non usare questa password ovunque, ma soltanto sui computer e i sistemi dei quali ci fidiamo a sufficienza[2].
In effetti, non solo si avrà accesso ai dati decifrati, ma rimarranno anche tracce della presenza del disco sul computer[3]. È per questo motivo che vi consigliamo di utilizzare il dispositivo cifrato montandolo su un sistema GNU/Linux a sua volta cifrato[4], oppure su un sistema Live amnesico come Tails[5].
Può essere un hard-disk, un disco SSD, una penna USB, una scheda SD, o anche solo di una parte di uno di questi dispositivi. È possibile infatti dividere un hard-disk o una penna USB in parti indipendenti, che chiameremo partizioni[6].
Da qui in poi parleremo di disco, dando per scontato, salvo contrordine, che il termine si riferirà sia a un hard-disk interno che a un hard-disk esterno, sia a qualsiasi tipo di periferica a memoria flash, come una penna USB, un disco SSD o una scheda SD.
Se vogliamo tenere su un disco un posto dove mettere dei dati

1 Cap. 5
2 Cap. 7
3 Cap. 2
4 Cap. 15
5 Cap. 14
6 Cap. 1

non confidenziali, e ai quali vogliamo poter accedere con dei computer di cui non ci fidiamo, possiamo dividere il disco in due partizioni:

- una partizione non cifrata, dove metteremo soltanto i dati non confidenziali, come ad esempio della musica, che potremo poi utilizzare in qualsiasi computer senza dover digitare la password;
- una partizione cifrata, con i dati confidenziali, che apriremo soltanto sui computer di cui ci fidiamo.

18.1 Cifrare un hard-disk con LUKS e `dm-crypt`

Spieghiamo adesso come cifrare un hard-disk attraverso i metodi standard previsto da GNU/Linux, che si chiamano `dm-crypt` e LUKS. Questo sistema adesso è ben integrato nell'ambiente base e quindi è possibile compere la maggior parte delle operazioni senza aver bisogno di particolari strumenti.

18.2 Altri strumenti che sconsigliamo

Esistono altri software crittografici come FileVault[7], che è integrato all'interno di Mac OS X, o BitLocker[8] per Windows

7 Una delle ultime analisi recenti di FileVault ha come data il 2012. Oltre ad essere vulnerabile agli stessi attacchi degli altri sistemi, FileVault ha qualche fragilità che vale la pena precisare: la passphrase che serve per cifrare spesso è identica alla password della sessione, in genere una password facile; il fatto di dover usare un'unica "password principale" offre il fianco a un ulteriore tipo d'attacco. Nonostante ciò, tenendo presente che offre un livello di protezione limitato, vale comunque la pena attivare FileVault se si dispone di un computer con Mac OS X.

8 Wikipédia, 2017, *BitLocker Drive Encryption* [https://it.wikipedia.org/]. wiki/BitLocker

– ma si tratta di software proprietari[9] – o anche VeraCrypt. Tuttavia quando si utilizza un software, foss'anche libero, su un sistema operativo proprietario[10], è di quest'ultimo che ci stiamo implicitamente fidando, poiché esso avrà necessariamente accesso ai dati decifrati.

18.3 In pratica

- Se abbiamo già usato questo hard-disk, potrebbe essere una buona idea quella di iniziare sovrascrivendo i dati[11].
- Se il disco da cifrare non ha abbastanza spazio libero, formattiamolo.
- In seguito, se vogliamo cifrare soltanto una parte del disco, dobbiamo creare una partizione in chiaro[12].
- Dopo di che non ci resta che configurarlo in modo che contenga dei dati cifrati[13].

A questo punto il disco è pronto da essere utilizzato.

18.4 Preparare un disco da cifrare

I software evolvono, per questo è vivamente consigliato utilizzare la versione più aggiornata di questa ricetta, che troverete in francese e in italiano sui siti della Guida https://guide.boum.org/ e https://numerique.noblogs.org/

Durata: circa 10 minuti.

9 Cap. 4
10 Cap. 1.4.1
11 Cap. 17
12 Cap. 18.5
13 *ibidem*

Da qui in poi parleremo sempre di disco, sapendo che intendiamo un hard-disk sia interno che esterno, una penna USB, una scheda SD o un disco SSD, a meno che non precisiamo.
La procedura che spiegheremo comporta la cancellazione di tutti i dati che si trovano sul disco[14]. Se abbiamo già dello spazio non partizionato sul nostro disco possiamo passare direttamente alla fase della cifratura[15].

18.4.1 Installare i pacchetti necessari

Per cifrare il nostro disco abbiamo bisogno di installare i pacchetti[16] `secure-delete`, `dosfstools` e `cryptsetup`. Se stiamo utilizzando Tails, questi pacchetti sono già installati.

18.4.2 Formattare il disco con l'utility dei dischi

Per aprire l'applicazione "Dischi" partiamo dalla vista d'insieme delle Attività: premere sul tasto ⊞ (⌘ su Mac), poi scrivere `disc` e cliccare su Dischi.
Nella finestra che si aprirà, la parte di sinistra mostra un elenco dei dischi presenti nel sistema; la parte di destra permette di effettuare delle operazioni.

Scegliere la periferica
A sinistra, c'è l'elenco dei dischi. Se il computer utilizzato contiene un sistema cifrato, vedremo anche i volumi cifrati del nostro sistema.

---

14 Potremmo anche utilizzare il programma GParted. Anche se è più difficile da usare rispetto all'utility dei dischi, ha il vantaggio di essere in grado di ridimensionare una partizione esistente senza cancellare i file che ci sono sopra.
15 Cap. 18.5
16 Cap. 16.3

Le icone e la grandezza, nonché il nome dei dischi, ci dovrebbero permettere di identificare quello che stiamo cercando.
Una volta trovato il disco, selezioniamolo nell'elenco. Le informazioni che compariranno nella parte destra della finestra dovrebbero confermarci che abbiamo scelto il disco giusto.

Smontare i volumi
Se il volume è montato, si dovrebbe vedere un'icona quadrata nella parte di destra, sotto la rappresentazione grafica del disco nell'elenco dei "Volumi".
Clicchiamo su quel bottone per smontare il volume. Se il disco contiene più volumi, selezioniamoli e smontiamoli con pazienza uno per uno.

Riformattare il disco

⚠ *Attenzione*: Formattare un disco significa perdere tutti i file che ci sono dentro.

Nella barra in alto del programma, clicchiamo sull'icona ☰, poi su "Formatta il disco"… Si aprirà una finestra che chiederà se confermare l'operazione di cancellazione dei dati e di formattazione del disco. In questo frangente, e sapendo già i limiti che riguardano questo argomento[17], scegliamo se cancellare o no i dati. Manteniamo l'opzione "Compatibile con tutti i sistemi e periferiche" nel "Partizionamento", e clicchiamo sul bottone "Formatta".
Ci viene chiesto se vogliamo davvero formattare la periferica. Prima di fare una scempiaggine, questo è il momento di controllare di aver scelto la periferica giusta. Se è tutto corretto, confermiamo cliccando su "Formatta".

---

17 Cap. 4

18.5 Creare una partizione non cifrata

I software evolvono, per questo è vivamente consigliato utilizzare la versione più aggiornata di questa ricetta, che troverete in francese e in italiano sui siti della Guida https://guide.boum.org/ e https://numerique.noblogs.org/

Durata: 2 minuti.

Se ne abbiamo bisogno, possiamo ora creare una partizione non cifrata dove mettere quei dati che non sono confidenziali, e che possiamo utilizzare su qualsiasi computer senza dover digitare la password.
Se invece vogliamo cifrare tutto il disco, possiamo passare direttamente al capitolo successivo.
Sempre nell'utility "Dischi", una volta selezionato il disco, clicchiamo nella parte destra sulla zona "Spazio disponibile" nello schema dei "Volumi". Clicchiamo poi lì sotto, sul simbolo +.
Nel campo dedicato scegliamo la dimensione che vogliamo per la partizione non cifrata. Lo spazio libero rimasto sarà quello che useremo poi per la partizione cifrata. Nel campo "Type", scegliere "Compatibile con tutti i sistemi e le periferiche (FAT)". Possiamo anche scegliere un nome per la partizione. Una volta fatto, clicchiamo su "Crea".

18.6 Creare una partizione cifrata

I software evolvono, per questo è vivamente consigliato utilizzare la versione più aggiornata di questa ricetta, che troverete in francese e in italiano sui siti della Guida https://guide.boum.org/ e https://numerique.noblogs.org/

Durata: 10 minuti + da qualche minuto a diverse ore per riempire lo spazio libero, a seconda delle dimensioni della partizione.

18.6.1 Creare la partizione cifrata

Sempre nell'utility "Dischi", una volta selezionato il disco, clicchiamo nella parte destra sulla zona "Spazio disponibile" nello schema dei "Volumi". Clicchiamo poi lì sotto, sul simbolo +.
Nel campo "Typer", scegliamo "Cifrato", compatibile con i sistemi Linux (LUKS + ext4), poi, nei due campi dedicati, scrivere una buona passphrase[18] per il volume cifrato. Possiamo anche dare un nome al volume. Una volta finito, clicchiamo su "Crea".

18.6.2 Riempire la partizione con dati casuali

Infine, dobbiamo riempire lo spazio vuoto dell'hard-disk con dati casuali. In questo modo renderemo meno evidente dov'è che si trovano i nostri dati, complicando la vita a chi vorrebbe provare a decifrarli.
Dentro lo schema dei "Volumi", troviamo "Partizione [...] LUKS" e selezioniamo il File System lì sotto. Sotto allo schema, clicchiamo su ▶.
In basso, nella finestra, dentro "Contenuto", c'è un link dopo "Montato su". Clicchiamo su questo link per aprire la cartella, poi seguiamo l'utility che serve a rendere irrecuperabili i dati già cancellati[19].
La procedura dura da qualche minuto a qualche ora, a secon-

18 Cap. 12
19 Cap. 17.7

da della dimensione dell'hard-disk e della sua velocità (per esempio, due ore per una penna USB da 4 GB).

18.6.3 Smontare correttamente l'hard-disk

Nel gestore dei file, clicchiamo sul simbolo ⏏, poi stacchiamo fisicamente il disco (nel caso si possa). Adesso il disco cifrato è utilizzabile.

18.7 Usare un dispositivo cifrato

I software evolvono, per questo è vivamente consigliato utilizzare la versione più aggiornata di questa ricetta, che troverete in francese e in italiano sui siti della Guida https://guide.boum.org/ e https://numerique.noblogs.org/

Durata: 2 minuti, qualche ora... o mai, a seconda della nostra capacità di ricordarci la passphrase.

Per permettere al sistema di accedere ai dati che si trovano su un dispositivo cifrato, È per fortuna necessario indicare una passphrase. Un'operazione più o meno semplice a seconda degli ambienti.

18.7.1 Con Debian (o altro GNU/Linux)

Su un sistema GNU/Linux con sopra un ambiente grafico configurato per aprire in automatico i media esterni, quando inseriremo un disco esterno cifrato, ci apparirà una finestra per chiederci la passphrase. Altrimenti, questa finestra apparirà nel momento in cui chiederemo al sistema di aprire quella

partizione cifrata, per esempio partendo dal gestore dei file.
Per chiudere la partizione cifrata, basterà smontare il disco come facciamo normalmente.

18.7.2 Con altri sistemi

Non conosciamo un modo semplice per acceder alla partizione cifrata del disco sotto Windows, o sotto Mac OS X. Anche se delle soluzioni esistono[20], è bene ricordare che si tratta di sistemi operativi proprietari, di cui non c'è alcuna buona ragione per fidarsi[21].
In questo caso la cosa migliore che possiamo fare, per mettere sul disco dei dati ai quali vogliamo accedere con dei computer dei quali non ci fidiamo, è creare una seconda partizione, non cifrata, sul disco, seguendo le istruzioni precedenti[22].

20 Per le vecchie versioni di Windows (fino a Vista), si poteva utilizzare FreeOTFE [sourceforge.net/projects/freeotfe.mirror/].

21 Cap. 4

22 Cap. 18.5

19 | Fare il backup dei dati

Fare un backup è un'operazione di base relativamente semplice: fondamentalmente dobbiamo copiare i file che non vogliamo perdere su un altro supporto, diverso da quello in cui si trovano attualmente.
Beninteso che se si tratta di dati su hard-disk o penne USB cifrati, è necessario che anche le copie risultino cifrate.
Ci sono altre due cose da non trascurare quando si mette in atto un buon piano di backup:

- definire un metodo per effettuare regolarmente i backup;
- controllare di tanto in tanto se i backup sono sempre ben leggibili.

Quest'ultimo aspetto è davvero importante. Perdere i dati originali è spesso una cosa dolorosa. Accorgersi in seguito che i backup non ci permettono di recuperare quello che abbiamo perso, trasforma il problema in catastrofe.
Allo stesso modo, è una buona idea anche quella di non conservare i backup nello stesso luogo in cui si trovano i dati originali. Altrimenti rischiamo di perderli, o di trovarli distrutti, entrambi.

19.1 Gestore dei file e backup cifrato

Realizzare dei backup è prima di tutto una questione di rigore e disciplina. Nei casi semplici possiamo utilizzare dei software specifici pensati per fare i backup, e accontentarsi semplicemente di effettuare le copie attraverso il gestore dei file.

19.1.1 Fare i backup

I software evolvono, per questo è vivamente consigliato utilizzare la versione più aggiornata di questa ricetta, che troverete in francese e in italiano sui siti della Guida https://guide.boum.org/ e https://numerique.noblogs.org/.

Durata: la prima volta, il tempo necessario a cifrare il dispositivo di archiviazione e quello per decidere quali file vogliamo salvare. In seguito il tempo dipenderà dalla quantità di dati da salvare.

La cifratura dei nostri backup sarà assicurata dalla cifratura del supporto di archiviazione esterno[1] (penna USB o hard-disk). Per effettuare le copie con regolarità e senza metterci troppo è consigliabile:

- avere da qualche parte un elenco dei file e delle cartelle da backuppare;
- farsi un piccolo calendario dei giorni in cui verranno fatti i backup, con delle caselline da spuntare via via.

Una buona pratica consiste nel creare una cartella con la data del backup, dove verranno copiati i dati. Questo permette sia di controllare facilmente se i vari backup sono stati fatti, sia di cancellare quelli vecchi.

19.1.2 Fare il restore di un backup

I software evolvono, per questo è vivamente consigliato utilizzare la versione più aggiornata di questa ricetta, che tro-

1 Cap. 18

verete in francese e in italiano sui siti della Guida https://guide.boum.org/ e https://numerique.noblogs.org/.

Durata: a seconda della quantità di dati da recuperare.

Nel caso in cui dovessimo perdere i dati originali, il restore si può fare facilmente: basta copiare i file da una parte all'altra, al contrario di come abbiamo fatto per il backup.

19.1.3 Assicurarsi che i backup siano sempre leggibili

I software evolvono, per questo è vivamente consigliato utilizzare la versione più aggiornata di questa ricetta, che troverete in francese e in italiano sui siti della Guida https://guide.boum.org/ e https://numerique.noblogs.org/.

Durata: circa 5 minuti + l'attesa della verifica

Se abbiamo effettuato il backup su un supporto di archiviazione esterno, dobbiamo prima di tutto attaccarlo al computer.
Il metodo più banale per assicurarsi che i backup siano sempre visibili è senza dubbio quello di simulare un restore. Procediamo quindi, ma potremmo incappare in un inconveniente... di dimensioni: bisogna avere abbastanza spazio libero a disposizione per copiare tutti i dati salvati in una cartella temporanea che poi cancelleremo.
C'è un altro metodo, forse meno facile da mettere in pratica, ma che non presenta questo inconveniente. Abbiamo bisogno di utilizzare un terminale[2].
Iniziamo a scrivere il comando (senza fare invio):

---

2 Cap. 11

```
find
```

Aggiungiamo uno spazio. Poi scriviamo la cartella che contiene i backup, cosa che possiamo fare con il mouse, trascinando l'icona della cartella e rilasciandola sul terminale. Una volta finito, ciò che viene fuori dovrebbe essere qualcosa di simile a:

```
find '/media/externe/sauvegardes'
```

Dobbiamo ora aggiungere la fine del comando in modo che il tutto assomigli a una cosa come:

```
find '/media/externe/sauvegardes' -type f -print0 |
xargs -0 cat > /dev/null
```

Il comando viene lanciato premendo Invio. La riga successiva dovrà rimanere vuota fino alla fine dell'operazione.
Dopo aver pazientato un po', ci verrà restituito il `$` del prompt e potremmo chiudere il terminale.
Se nel frattempo sono apparsi dei messaggi di errore tipo "Input/Output error" vuol dire che il backup è corrotto. Come regola generale, bisogna allora sbarazzarsi del supporto di archiviazione (CD, DVD, penna USB o hard-disk), prenderne un altro e rifare da capo il backup.
Nota bene: entrambi i metodi condividono il difetto di non verificare l'integrità dei dati[3]. Poterlo fare implica il dover passare a dei software di backup più complessi.

19.2 Utilizzare Déjà Dup

Durata: 5 minuti per installare il software.

3 Cap 5.2

Magari preferiamo usare un software specifico per i backup. Uno di questi, chiamato *Déjà Dup*, ha il vantaggio di essere facile da usare, e quello di poter creare dei backup cifrati. Questi backup sono “incrementali”, ovvero i file che sono rimasti immutati dal backup precedente non vengono copiati un’altra volta, ed è possibile accedere alle versioni dei file per come erano in ciascun backup.
Ciò che lo rende semplice può però rivelarsi anche un limite: il programma è in grado di gestire una sola configurazione alla volta. Non possiamo quindi backuppare cartelle diverse su supporti diversi a intervalli temporali diversi. È uno strumento ideale per salvare l’essenziale contenuto nella nostra cartella personale, ma niente di più.
Non viene rilasciato di default con il sistema, quindi per usarlo è necessario installare il pacchetto[4] Debian `déjà-dup`.

19.2.1 Fare un backup

I software evolvono, per questo è vivamente consigliato utilizzare la versione più aggiornata di questa ricetta, che troverete in francese e in italiano sui siti della Guida https://guide.boum.org/ e https://numerique.noblogs.org/.

Durata: 15 minuti circa per la configurazione, da qualche minuto a diverse ore per il backup, a seconda della dimensione di ciò che vogliamo copiare.

Apriamo l’applicazione Backups partendo dalla vista d’insieme delle Attività: premiamo il tasto ⊞ (⌘su Mac), poi scriviamo `back` e clicchiamo su “Backups”.
All’avvio l’interfaccia non corrisponderà a ciò che vorremmo

4 Cap. 16.3

visualizzare. Per rimediare, clicchiamo nel menu di sinistra su "Cartelle da salvare" poi, sempre nel menu, su "Panoramica". Adesso l'interfaccia dovrebbe mostrare la vista d'insieme. Dentro "Panoramica" troviamo due pulsanti, uno per "Ripristinare" dei file di un precedente backup, l'altro per "Eseguire il backup". Ma prima di eseguire un backup, bisogna configurare cosa vogliamo salvare e dove.

1. Nel menu di sinistra, clicchiamo su "Cartelle da salvare" per visualizzare l'elenco delle cartelle da includere nel backup. Possiamo lasciare "Home", che è la scelta predefinita e sufficiente per la maggior parte dei casi.
2. Dentro "Cartelle da ignorare", possiamo selezionare le cartelle da ignorare che contengono file spesso voluminosi, ma più facili da ritrovare, come video e musica.
3. Dentro "Posizione" di archiviazione scegliamo il luogo in cui salvare. Per archiviare i backup su un disco esterno, attacchiamo il disco in questione al computer, poi nell'elenco "Posizione di archiviazione" clicchiamo su Dischi locali e poi selezioniamo la periferica che vogliamo.
4. Se vogliamo effettuare automaticamente questi backup, clicchiamo su "Pianificazione" per scegliere la frequenza dei backup e la durata della conservazione dei dati.
5. Adesso possiamo ritornare a "Panoramica". Nel caso in cui abbiamo scelto un piano di backup automatico, attiviamo l'interruttore on/off sulla barra del titolo. Altrimenti clicchiamo su "Esegui backup adesso". Si aprirà una nuova finestra che ci chiederà una password per cifrare[5] il nostro nuovo backup[6]. Una volta confermata la password,

5 Cap. 12
6 Se il dispositivo esterno è cifrato, possiamo eventualmente decidere di non cifrare i file backuppati. Sarà una passphrase in meno da inventarsi e da ricordarsi. Perderemo però la possibilità di compartimentare gli accessi, nel caso in cui il dispositivo esterno ci serva ad altro oltre che ai backup.

clicchiamo su "Continua" per eseguire il backup.

6. Possiamo quindi chiudere backup. La prossima volta, se i parametri non sono cambiati, basterà mettere la password e il backup verrà aggiornato.

Se ne abbiamo bisogno, possiamo modificare in seguito questi parametri lanciando di nuovo Backup.
Quando i backup programmati sono attivi ed è arrivato il momento di fare il prossimo backup, Déjà Dup fa comparire un messaggio di notifica per avvertirci che effettuerà il prossimo backup non appena il dispositivo esterno verrà attaccato al computer. E in quel momento, si aprirà automaticamente una finestra per chiederci la passphrase necessaria per aggiornare i backup.

19.2.2 Ripristinare un backup

I software evolvono, per questo è vivamente consigliato utilizzare la versione più aggiornata di questa ricetta, che troverete in francese e in italiano sui siti della Guida https://guide.boum.org/ e https://numerique.noblogs.org/.

Durata: 5 minuti per la configurazione, da qualche minuto a qualche ora per il ripristino, a seconda della dimensione dei nostri dati.

Dalla vista d'insieme delle attività, aprire backup: premere ⊞ (⌘ su Mac), poi scrivere `back` e cliccare su "Backup". L'operazione di ripristino parte quando si clicca su "Ripristina".
Se questa è la prima volta che utilizziamo Backup (se, per esempio, lo stiamo usando per recuperare le nostre cartelle personali dopo la perdita di un hard-disk), ci verrà chiesto di indicare la cartella dove sono stati salvati i backup. Altrimen-

ti attingeremo alla cartella configurata in precedenza. Dopo una breve attesa backup ci chiederà di scegliere, guardando la data dei file, il backup che vogliamo ripristinare. Clicchiamo su "Avanti".
A questo dovremo indicare la cartella dove verranno salvati i file ripristinati dal backup. Possiamo sia ripristinare i file dov'erano in origine (questo sovrascriverà eventuali file con la versione che si trovava nel backup), sia ripristinare dentro una specifica cartella differente. Clicchiamo su "Avanti".
Infine, apparirà un'ultima schermata che ci riepiloga i parametri di questo ripristino. Clicchiamo su "Ripristina", se necessario si aprirà una finestra per chiederci la password di amministratore (se ne potrebbe avere bisogno, per esempio, per ripristinare i permessi di alcuni file). Se il backup era cifrato, Déjà Dup ci chiederà la passphrase. Clicchiamo su "Continua" e comincerà la scrittura dei file provenienti dal backup.

19.2.3 Assicurarsi che i backup continuino ad essere leggibili

I software evolvono, per questo è vivamente consigliato utilizzare la versione più aggiornata di questa ricetta, che troverete in francese e in italiano sui siti della Guida https://guide.boum.org/ e https://numerique.noblogs.org/.

Durata: da qualche minuto a qualche ora, a seconda delle dimensioni del nostro backup.

Il funzionamento incrementale di Déjà Dup assicura già in modo superficiale che i precedenti backup siano leggibili. Ma questo non costituisce una garanzia...
Purtroppo al momento il miglior metodo disponibile con Déjà Dup per assicurarsi di poter ripristinare i propri dati è fare un

ripristino dentro a una cartella temporanea che poi cancelleremo. È un metodo tutt'altro che pratico, visto che occorre avere accesso a un hard-disk cifrato abbastanza capiente.

20 | Condividere un segreto

I software evolvono, per questo è vivamente consigliato utilizzare la versione più aggiornata di questa ricetta, che troverete in francese e in italiano sui siti della Guida https://guide.boum.org/ e https://numerique.noblogs.org/.

Durata: circa un'ora.

Talvolta abbiamo bisogno di condividere un segreto in tanti, senza che ciascuno conosca il segreto per intero.
Non è difficile, perché diverse tecniche crittografiche sono state inventate proprio per fare questo. Tutte quante, anche se con calcoli matematici diversi tra loro, permettono di scomporre un segreto in tanti pezzetti, che potrà essere poi ricostruito riunendone alcuni.

20.1 Condividere una passphrase

L'esempio più pratico è quello di condividere la passphrase di un supporto cifrato[1].
Questo passaggio dovrà idealmente essere fatto a partire da un sistema Live[2], in modo da non lasciare tracce del segreto che vogliamo condividere.

20.1.1 Installare il pacchetto necessario

Per spezzettare il segreto, utilizzeremo il programma `ssss-split`. Possiamo trovare questo software tra quelli forniti da

1 Cap. 18
2 Cap. 14

Tails, ma se se invece vogliamo servircene su una Debian cifrata, dobbiamo installare il pacchetto Debian *ssss*[3].
Gli strumenti contenuti dentro il pacchetto ssss vanno utilizzati a linea di comando. Ogni operazione dovrà quindi essere effettuata all'interno di un terminale[4], da semplice utente.

20.1.2 Generare una passphrase casuale

Nel nostro caso, nessuno deve essere in grado di ricordare né indovinare la passphrase che utilizzeremo per la cifratura del supporto. Dobbiamo quindi generare una passphrase casuale attraverso il comando:

```
head -c 32 /dev/random | base64
```

Il computer risponderà qualcosa tipo:

```
7rZwOOu+8v1stea98OuyU1efwNzHaKX9CuZ/TK0bRWY=
```

Se vogliamo una passphrase con più o meno di 32 caratteri, basterà sostituire a 32 il numero di caratteri che vogliamo. Selezioniamo il risultato e copiamolo negli appunti.

20.1.3 Spezzettare il segreto

Prima di spezzettare il segreto, dobbiamo decidere in quante parti vogliamo scomporlo e quante di queste parti devono essere necessarie per ricostruirlo.
Poi, sempre con l'aiuto del nostro terminale, dobbiamo utilizzare `ssss-split` nel modo seguente:

---

3 Cap. 16.3
4 Cap. 11

```
ssss-split -t numero_di_parti_necessarie -n nume-
ro_di_parti_totali
```

`numero_di_parti_necessarie` è il numero di parti che devono necessariamente esserci per ritrovare la passphrase iniziale. `numero_di_parti_totali` corrisponde al numero di parti nel quale la passphrase verrà spezzettata. Se stiamo utilizzando una distribuzione Live ignoriamo tranquillamente l'eventuale messaggio `WARNING: couldn't get memory lock`.
Al momento in cui ci viene chiesto il segreto, lo incolliamo dagli appunti. Poi diamo invio per confermare il comando.
Ogni persona che deve condividere il segreto, dovrà conservare una delle righe mostrate in seguito. Tutta intera, *così com'è*: copiando anche la prima cifra seguita dal trattino.
Ecco un esempio con la passphrase casuale che abbiamo generato prima, condivisa tra sei persone e che necessita di almeno tre di loro per essere ricostruita:

```
$ ssss-split -t 3 -n 6
Generating shares using a (3,6) scheme with dynamic
security level.
Enter the secret, at most 128 ASCII characters:
Using a 352 bit security level.
1-b8d576a1a8091760b18f125e12bb6f
2b1f2dd9d93f7072ec69b129b27bb8 e
97536ea85c7f6dcee7b4399ea49
2-af83f0af05fc207e3b466caef30ec4
d39c060800371feab93594350b7699 a
8db9594bfc71ed9cd2bf314b738
3-4718cb58873dab22d24e526931b061
a6ac331613d8fe79b2172213fa767c a
a57d29a6243ec0e6cf77b6cbb64
4-143a1efcde7f4f5658415a150fcac6
da04f697ebfeb9427b59dca57b50ec 7
```

```
55510b0e57ccc594e6b1a1eeb04
5-fca1250b5cbec40ab14964d2cd7463
af34c389f81158d1707b6a838a5009 7
7d957be38f83e8eefb79266e74a
6-ebf7a305f14bf3143b801a222cc
1c8 57b7e8582119374925274f9f335d28 3
677f4c002f8d68bcce722ebba1f
```

20.1.4 Creare il supporto cifrato

Adesso potremo creare il supporto cifrato[5]. Al momento di indicare la passphrase, potremo copiare il contenuto dagli appunti, come abbiamo fatto prima, o scrivercela tenendocela sotto gli occhi.

20.2 Ricostruire la passphrase

Per ricostruire la passphrase, è necessario disporre del numero minimo di parti che avevamo deciso al momento dello spezzettamento.
Idealmente questa parte dovrebbe essere fatta all'interno di un sistema Live[6] in modo da non lasciare traccia del segreto condiviso.

20.2.1 Installare i pacchetti necessari

Come prima, se il programma non è disponibile sul sistema dovremo installare il pacchetto *ssss*[7] e aprire un terminale.

5 Cap. 18
6 Cap. 14
7 Cap. 16.3

20.2.2 Ricostruire il segreto

Per ricostruire il segreto, utilizzeremo il programma `ssss-combine`. Bisogna indicargli il numero di parti che abbiamo a disposizione:

```
ssss-combine -t numero_di_parti_a_nostra_disposi-
zione
```

Il programma in seguito ci chiede di indicare le parti che abbiamo a disposizione. Le scriviamo una per una, dando invio ogni volta. Se tutto è andato bene, il programma mostrerà la passphrase completa.
Per riprendere l'esempio precedente, avremo:

```
$ ssss-combine -t 3
Enter 3 shares separated by newlines:
Share 3: 4-143a1efcde7f4f5658415a150fcac6
da04f697ebfeb9427b 59dca57b50ec755510b0e57ccc594e
6b1a1eeb04
Share 3: 2-af83f0af05fc207e3b466caef30ec4
d39c060800371feab9 3594350b7699a8db9594bfc71ed9cd
2bf314b738
Share 3: 6-ebf7a305f14bf3143b801a222cc1c8
57b7e8582119374925 274f9f335d283677f4c002f8d68bcc
e722ebba1f
Resulting secret:
7rZwOOu+8v1stea98OuyU1efwNzHaKX9CuZ/TK0bRWY=
```

⚠ *Attenzione*: se abbiamo scritto male una delle parti, l'errore che viene fuori non è molto esplicito:

```
$ ssss-combine -t 3
Enter 3 shares separated by newlines:
```

```
Share 3: 4-143a1efcde7f4f5658415a150fcac6
da04f697ebfeb9427b 59dca57b50ec755510b0e57ccc594e
6b1a1eeb04
Share 3: 2-af83f0af05fc207e3b466caef30ec4
d39c060800371feab9 3594350b7699a8db9594bfc71ed9cd
2bf31ab738
Share 3: 6-ebf7a305f14bf3143b801a222cc1c8
57b7e8582119374925 274f9f335d283677f4c002f8d68bcc
e722ebba1f
Resulting secret: ......L.fm.....6 _....v..w.a....
[....zS.....
WARNING: binary data detected, use -x mode instead.
```

20.2.3 Aprire il supporto cifrato

Una volta ottenuta la passphrase, possiamo utilizzare il copia/incolla per sbloccare il supporto cifrato, oppure ricopiarla a mano.

21 | Utilizzare i checksum

I software evolvono, per questo è vivamente consigliato utilizzare la versione più aggiornata di questa ricetta, che troverete in francese e in italiano sui siti della Guida https://guide.boum.org/ e https://numerique.noblogs.org/.

Durata: da 5 a 10 minuti

Nel capitolo 5 abbiamo evocato i checksum, dei "numeri" che permettono di verificare l'integrità di un file (o di altri dati). Il principio è che sia praticamente impossibile avere un checksum identico per due file diversi. Se Alice dice a Betty in una lettera che il programma che può scaricarsi dal suo sito ha come checksum HA256 `171a0233a4112858db23621dd5ffa-31d269cbdb4e75bc206ada58ddab444 651f` e se il file che Betty ha ricevuto ha lo stesso checksum, è praticamente sicuro che nessuno ha falsificato il programma nel mentre, e quindi Betty può eseguire il programma senza troppi timori.
Esistono diversi algoritmi per calcolare checksum. Tra questi:

- MD5 ad oggi non è più sicuro ed è deprecato;
- SHA1 è molto utilizzato, ma sta per essere dismesso. Tocca abbandonarlo;
- SHA224, SHA256, SHA384 e SHA512 al momento sono sicuri. Qui useremo SHA256, ma gli stessi metodi funzionano anche con gli altri algoritmi.

21.1 Ottenere il checksum di un file

Sia che vogliate verificare l'integrità di un file o che vogliate permettere al vostro corrispondente di farlo, dovrete calcolare

il checksum[1] del file. Si può utilizzare uno strumento grafico oppure il terminale, in questo caso non spiegheremo i dettagli per l'uso del terminale.

21.1.1 Installare i programmi necessari

Se il pacchetto `nautilus-gtkhash` non è ancora installato, installiamolo[2], poi riavviamo il computer. Su Tails questo pacchetto è installato di default.

21.1.2 Calcolare il checksum

Aprire il gestore dei file a partire dalla vista d'insieme delle Attività: premere il tasto ⊞ (⌘su Mac), poi scrivere `fil` e cliccare sul Gestore dei file.
Selezionare il file del quale vogliamo ottenere i checksum, poi clicchiamoci col destro. Nel menu contestuale che apparirà scegliamo "Proprietà", poi "Impronte" ("Digest").
Ci sono diverse funzioni hash, di cui tre sono selezionate di default: MD5, SHA1 e SHA256. Se ci occorre un checksum diverso da questi spuntiamo la casella corrispondente. Clicchiamo su "Hash". Nella colonna "Digest" appariranno i checksum.

21.2 Verificare l'integrità di un file

È importante che il checksum di un file originale venga ottenuto attraverso un canale sicuro, diverso da quello attraverso il quale abbiamo ottenuto il file. Per esempio, se abbiamo sca-

1 Cap. 5.2
2 Cap. 16.3

ricato il file, sarebbe meglio ricevere il checksum via mail, per telefono o (sicuramente l'opzione migliore) di persona.
Allo stesso modo, se dobbiamo permettere ad altre persone di verificare l'integrità di un file, sarà meglio fargli pervenire il checksum con questi metodi.
Attraverso uno di questi metodi otteniamo il checksum della nostra copia del file. Facciamo attenzione a utilizzare lo stesso algoritmo di quello che ha utilizzato il nostro corrispondente. Se abbiamo utilizzato SHA1 e l'altro ha utilizzato SHA256, ovviamente i checksum non corrisponderanno. Se il nostro corrispondente ci propone vari checksum, cerchiamo di scegliere l'algoritmo più difficile da rompere[3].
Verifichiamo che i due checksum siano gli stessi (è un po' lungo e fastidioso, spesso è più comodo farlo in due, oppure copiarli uno sotto l'altro in un file di testo).

---

3 Cap. 21

22 | Installare e utilizzare un sistema virtuale

Lo scopo di questo insieme di ricette è quello di utilizzare un sistema operativo virtuale (che chiameremo "ospitato") all'interno del nostro sistema GNU/Linux (che chiameremo "ospitante"): tutto ciò viene chiamato "virtualizzazione". Di questa tecnologia, così come della policy di sicurezza per utilizzarla, parleremo più avanti nell'esempio che spiega come lavorare su un documento sensibile sotto Windows[1].

⚠ *Attenzione*: nelle edizioni precedenti della Guida abbiamo consigliato di utilizzare il programma VirtualBox, che però adesso non è più disponibile su Debian. Se prima usavamo quel software, dovremo installare di nuovo la nostra macchina virtuale e migrarla da VirtualBox al Gestore delle macchine virtuali. Non documentiamo questa procedura in questa guida, ma possiamo comunque lanciarci nell'avventura seguendo le istruzioni che si trovano sul web[2].

22.1 Installare il gestore di macchine virtuali

I software evolvono, per questo è vivamente consigliato utilizzare la versione più aggiornata di questa ricetta, che troverete in francese e in italiano sui siti della Guida https://guide.boum.org/ e https://numerique.noblogs.org/.

Durata: circa un quarto d'ora

1 Cap. 9.6
2 Malte Gerken, 2017, *Migrate a VM from VirtualBox to libvirt* [https://www.maltegerken.de/blog/2017/01/migrate-a-vm-from-virtualbox-to-libvirt/].

22.1.1 Il principio

L'obiettivo di questa ricetta è di installare il Gestore di macchine virtuali, un programma che ci permetterà di far funzionare un sistema Windows virtuale all'interno del nostro sistema Debian GNU/Linux.

22.1.2 Installare il Gestore di macchine virtuali

Il primo passo quello di installare il pacchetto[3] `virt-manager`.

22.1.3 Verificare l'installazione

Per lanciare il Gestore di macchine virtuali, apriamo la vista d'insieme delle Attività premendo il tasto ⊞ (⌘su Mac), poi scriviamo `virt` e clicchiamo su "Gestore delle macchine virtuali". A questo punto ci verrà chiesta la password di amministrazione, è normale.

22.2 Installare un Windows virtuale

↻ I software evolvono, per questo è vivamente consigliato utilizzare la versione più aggiornata di questa ricetta, che troverete in francese e in italiano sui siti della Guida https://guide.boum.org/ e https://numerique.noblogs.org/.

◷ Durata: circa 20 minuti, più il tempo necessario a installare Windows (da mezz'ora a un'ora).

3 Cap. 16.3

Prima di tutto, muniamoci di un CD di installazione della versione di Windows appropriata, e inseriamolo nel lettore CD/DVD. Se dovesse aprirsi automaticamente una finestra che mostra il contenuto del CD, chiudiamola o ignoriamola.

22.2.1 Creare una nuova macchina virtuale

Per lanciare il Gestore di macchine virtuali, apriamo la vista d'insieme delle Attività premendo il tasto ⊞ (⌘su Mac), poi scriviamo `virt` e clicchiamo su "Gestore delle macchine virtuali". Il programma si avvierà, a questo punto occorrerà mettere la password che ci chiede e autenticarsi. Clicchiamo sul menu "File", poi "Nuova macchina virtuale" e seguiamo i cinque passi della procedura guidata.

- Primo passo: Selezionare il "Media di installazione locale (immagine ISO o CD-ROM)".
- Secondo passo: "Use CD-ROM or DVD" è la scelta predefinita, altrimenti selezioniamola. Se il tipo di Sistema Operativo e la sua versione (OS Type e Version) non vengono riconosciuti correttamente, spuntare "Automatically detect operating system based on install media" per sceglierli in modo manuale.
- Terzo passo: Nella finestra successiva, indichiamo quanta RAM e quante CPU vogliamo dedicare alla macchina virtuale. Ecco i parametri minimi raccomandati per l'ultima versione di Windows:

  Windows 7: *RAM 1024 MiB, CPU 1*
  Windows 8: *RAM 2048 MiB, CPU 1*
  Windows 10: *RAM 2048 MiB, CPU 1*

- Quarto passo: Scegliamo le dimensioni dell'immagine virtuale. Visto che vogliamo ospitare Windows, le dimensioni dovranno essere adeguate: minimo 20 GB.
- Quinto passo: Indichiamo un Nome per la macchina virtuale e poi spuntiamo "Customize configuration before install".
- Infine clicchiamo su "Finish".

Se compare un messaggio che lamenta che la rete virtuale non è attiva, clicchiamo su "Yes" per avviarla, altrimenti non è possibile passare al passo successivo.
Si aprirà una finestra, selezioniamo nella colonna dell'hardware la scheda di rete (NIC) che gestirà l'interfaccia di rete virtuale e poi clicchiamo su "Apply". Nella finestra di conferma scegliamo "Yes". La macchina virtuale a questo punto è isolata dalla rete.
Aggiungiamo adesso un canale (channel) necessario per condividere file tra il sistema originale (ospitante) e il sistema ospitato. Per farlo clicchiamo sul tasto in basso a sinistra "Add hardware". Si aprirà una finestra, dove dobbiamo cliccare su "Channel" scegliendo nell'elenco di sinistra. Nel menu a tendina del "Name" selezioniamo "org.spice-space.webdav.0", poi clicchiamo su "Finish".
Clicchiamo su "Begin installation" in alto a sinistra, per lanciare l'installazione di Windows.

22.2.2 Installare Windows sulla macchina virtuale

Il sistema virtuale viene avviato dal lettore CD/DVD che gli abbiamo indicato e l'installazione ha inizio. Non entreremo nei dettagli del processo, che dipendono dalla nostra versione di Windows, ma occorre precisare:

- Non mettere informazioni personali come il nome e l'organizzazione anche se ci vengono chieste. Mettere per esempio "user".
- Dovendo inserire un numero di serie di Windows, questo verrebbe attribuito ufficialmente a noi e creerebbe quindi un riferimento.
- Potrebbe comparire un messaggio di errore durante la configurazione della rete. È un buon segno: avevamo disattivato la rete nella macchina virtuale.

Una volta terminata l'installazione, spegniamo Windows cliccando sul menu "Virtual machine" → "Shut down" → "Shut down". Dentro la finestra della macchina virtuale, clicchiamo sul menu "View" → "Details". Nell'elenco di sinistra scegliamo "IDE CD-ROM 1", poi dentro "Source path" clicchiamo su "Disconnect".
Per espellere il CD/DVD, apriamo la vista d'insieme delle Attività premendo il tasto ⊞ (⌘ su Mac), poi scriviamo `fil` e clicchiamo su "Gestore dei file". Nell'elenco di sinistra, nella finestra che si apre, troviamo CD/DVD e clicchiamo sull'icona ⏏ corrispondente.

22.2.3 Preparare i guest tools per il gestore di macchine virtuali

Esistono dei driver specifici che consentono di migliorare l'interazione tra il Gestore di macchine virtuali e il sistema Windows ospitato, grazie a una tecnologia chiamata SPICE: si tratta di alcuni strumenti (guest tools) e di un servizio di condivisione file. Dentro il sistema ospitante, scarichiamo l'installer Windows per i guest tools SPICE (http://dacato.vado.li). Per verificare il file scaricato possiamo scaricare la sua firma (http://loputu.vado.li).

Ora andiamo a scaricare l'installer webDAV per SPICE (http://vivube.vado.li). Clicchiamo sul link che corrisponde all'ultima versione dell'architettura della nostra macchina virtuale. Il nome finisce con "-x86-latest.msi" per un Windows a 32 bit o con "-64-latest.msi" per un Windows a 64 bit.
Per trasferire i due installer dalla macchina ospitante al Windows ospitato, dobbiamo preparare con il software *Brasero* un'immagine in formato ISO che contenga i due file. Per lanciare Brasero apriamo la vista d'insieme delle Attività premendo il tasto ⊞ (⌘ su Mac), poi scriviamo `bra` e clicchiamo su "Brasero".
Scegliamo Data project. Clicchiamo sull'icona + e aggiungiamo i file che abbiamo appena scaricato: "spice-guest-tools" e "spice-webdavd".
Nel menu a tendina in fondo alla finestra, scegliamo "Image file" e poi clicchiamo su "Burn". Come nome del file per esempio scegliamo "guest-tools-Windows" e clicchiamo su "Create image". Una volta creata l'immagine chiudiamo Brasero.

22.2.4 Installare i guest tools per il gestore di macchine virtuali

Torniamo nel Gestore delle macchine virtuali e condividiamo l'immagine ISO che abbiamo appena creato con la macchina virtuale, seguendo la ricetta "Condividere un CD con il sistema virtuale"[4].
Adesso, sempre nel Gestore delle macchine virtuali, avviamo la macchina virtuale cliccandoci sopra con il destro e cliccando su Open. Nella nuova finestra che si apre andiamo nel menu "Virtual machine" e clicchiamo su "Start".
Una volta all'interno del sistema Windows virtuale, apria-

4 Cap. 22.5

mo il CD-ROM virtuale e clicchiamo due volte sul file `spice-guest-tools`. Ogni volta che Windows chiede se vogliamo autorizzare un programma sconosciuto (ovvero non verificato da Microsoft), accettiamo. Accettiamo anche tutte le altre richieste del programma di installazione, cliccando su “Avanti”. Facciamo la stessa cosa con `spice-webdavd`.
Adesso è possibile copia-incollare del testo dalla macchina ospitante alla macchina virtuale ospitata e viceversa. È anche possibile modificare la visualizzazione della macchina virtuale in proporzione alle dimensioni della finestra che ospita Windows. Clicchiamo sul menu “View” → “Scegliere” la risoluzione e selezionare “Auto-resize guest display”.
L’installazione del sistema Windows virtuale è finita.

22.3 Fare uno snapshot di una macchina virtuale

I software evolvono, per questo è vivamente consigliato utilizzare la versione più aggiornata di questa ricetta, che troverete in francese e in italiano sui siti della Guida https://guide.boum.org/ e https://numerique.noblogs.org/.

Durata: 5 minuti

Per seguire il metodo che consente di lavorare su un documento sensibile sotto Windows[5], potremmo avere bisogno di salvare lo stato di una macchina virtuale. Per farlo utilizziamo il gestore delle istantanee per macchine virtuali, in inglese *snapshot*.

Apriamo la vista d’insieme delle Attività premendo il tasto ⊞ (⌘ su Mac), poi scriviamo `virt`, clicchiamo su “Gestore delle

5 Cap. 9.6

macchine virtuali” e inseriamo la password. Selezioniamo la macchina virtuale giusta e clicchiamo su “Open”. Se è già accesa, spegniamola cliccando sul menu “Virtual machine” → “Shut down” → “Shut down”.
Clicchiamo su “View” → “Snapshot”. Nell’elenco di sinistra clicchiamo sul pulsante + in basso. Nella finestra che appare indichiamo il Nome dell’istantanea, per esempio “il mio Windows”. Eventualmente aggiungiamo una “Descrizione” e poi clicchiamo su “Finish”.

22.4 Ripristinare lo stato di una macchina virtuale a partire da uno snapshot

I software evolvono, per questo è vivamente consigliato utilizzare la versione più aggiornata di questa ricetta, che troverete in francese e in italiano sui siti della Guida https://guide.boum.org/ e https://numerique.noblogs.org/.

Durata: dipende dalle dimensioni del disco.

Lo scopo di questa ricetta è quello di ripristinare lo stato di una macchina virtuale a partire da uno snapshot creato in precedenza[6]. Così facendo sarà possibile utilizzarla per un nuovo progetto, come raccomanda il metodo consigliato per lavorare su un documento sensibile sotto Windows[7].

22.4.1 Visualizzare gli snapshot

Cominciamo con l’aprire la vista d’insieme delle Attività premendo il tasto ⊞ (⌘ su Mac), poi scrivendo `virt`, cliccan-

6 Cap. 22.4
7 Cap. 9.6

do su “Gestore delle macchine virtuali” e inserendo la password. Selezioniamo la macchina virtuale giusta e clicchiamo su “Open”. Dentro la finestra successiva clicchiamo sul menu “View” e selezioniamo “Snapshot”.

22.4.2 Scegliere e ripristinare uno snapshot

Selezioniamo lo snapshot giusto a partire dal quale vogliamo ripristinare lo stato della macchina (per esempio “Il mio Windows”). Clicchiamo sul pulsante ▶, in basso a sinistra. Apparirà una nuova finestra che ci chiederà se siamo sicuri di voler eseguire lo snapshot selezionato. Eseguirlo comporta che ogni modifica effettuata sulla macchina virtuale dopo la creazione di questo snapshot andrà perduta. Se siamo sicuri della nostra scelta clicchiamo su “Yes”, altrimenti su “No”.
Il gestore della macchina virtuale comincerà a ripristinare lo stato della macchina virtuale com’era nel momento in cui è stato catturato lo snapshot.

22.5 Condividere un CD o un DVD con un sistema virtuale

↻ I software evolvono, per questo è vivamente consigliato utilizzare la versione più aggiornata di questa ricetta, che troverete in francese e in italiano sui siti della Guida https://guide.boum.org/ e https://numerique.noblogs.org/.

🕓 Durata: 10 minuti circa

Questa operazione è necessaria quando vogliamo installare sul sistema Windows virtuale dei software che abbiamo su un CD/DVD o su un’immagine ISO.

Cominciamo con l'aprire la vista d'insieme delle Attività premendo il tasto ⊞ (⌘ su Mac), poi scrivendo `virt`, cliccando su "Gestore delle macchine virtuali" e inserendo la password.
Selezioniamo la macchina virtuale Windows con la quale vogliamo condividere un CD o un DVD. Scegliamo la visualizzazione dettagliata della macchina virtuale cliccando sul menu "View" → "Details". Nell'elenco dell'hardware a sinistra, selezioniamo "IDE CD-ROM 1" e clicchiamo su "Connect".
A questo punto ci sono due scelte:

- se vogliamo condividere un CD o un DVD fisico con la macchina virtuale, inseriamolo nel lettore e aspettiamo qualche istante. Poi scegliamo "CD-ROM" o "DVD";
- se vogliamo invece condividere un'immagine ISO, scegliamo "ISO image location", poi clicchiamo su "Browse". Nella finestra che si apre scegliamo l'immagine ISO.

In entrambi i casi finiamo premendo su "Apply". Torniamo a Windows con "View" → "Console". A questo punto Windows dovrebbe rilevare il CD inserito. Se non fosse così possiamo cercarlo dentro Risorse del computer (nelle versioni più nuove di Windows "questo PC"). Se al primo colpo non va, riproviamo da capo.
Quando abbiamo finito di usare il CD espelliamolo da dentro Windows, poi ritorniamo alla visualizzazione dettagliata della macchina virtuale con "View" → "Details", selezioniamo "IDE CD-ROM 1" e clicchiamo su "Disconnect".

22.6 Condividere una cartella con un sistema virtuale

↻ I software evolvono, per questo è vivamente consigliato utilizzare la versione più aggiornata di questa ricetta, che tro-

verete in francese e in italiano sui siti della Guida https://guide.boum.org/ e https://numerique.noblogs.org/.

Durata: circa 10 minuti

Dato che il Windows ospitato non ha i permessi di uscire dalla sua scatola per andarsi a cercare da solo i file, potrebbe essere necessario farglieli avere "dall'esterno". Vediamo come.

⚠ *Attenzione*: imparare a utilizzare questo sistema di condivisione, potrebbe anche voler dire volerlo configurare per dargli accesso a tutti i dischi collegati al sistema ospitante: *sarebbe una pessima idea*, che annienterebbe in un colpo solo ogni policy di sicurezza.

Creare una cartella dedicata a questo scopo nel sistema ospitante

Apriamo la vista d'insieme delle Attività premendo il tasto ⊞ (⌘ su Mac), poi scrivendo `fil` e cliccando su "Gestore dei file". Scegliamo dove vogliamo che stia questa cartella di condivisione. Per esempio: nella cartella dei documenti clicchiamo sull'icona ≡ poi su "Crea cartella" e diamogli un nome evocativo ("cartella leggibile da Windows", per esempio). Dentro questa cartella metteremo i file che vogliamo trasferire a Windows.

Installare il remote viewer

Attualmente il Gestore di macchine virtuali non permette l'attivazione della condivisione delle cartelle. È necessario utilizzare il software di visualizzazione remota (remote viewer). Il passo successivo è quindi quello di installare il pacchetto[8] `virt-viewer`.

8 Cap. 16.3

Attivare la condivisione della cartella
Per attivare la condivisione della cartella, dobbiamo per prima cosa avviare la macchina virtuale Windows attraverso il Gestore di macchine virtuali.
Apriamo la vista d'insieme delle Attività premendo il tasto ⊞ (⌘ su Mac), poi scriviamo `virt`, clicchiamo su "Gestore delle macchine virtuali" e inseriamo la password.
Nella finestra del Gestore delle macchine virtuali, clicchiamo col destro sulla macchina virtuale giusta (per esempio il nostro Windows) e clicchiamo su "Start".
La macchina virtuale si avvierà, ma il suo schermo non sarà visibile. Per accederci utilizzeremo il software di remote view.
Apriamo la vista d'insieme delle Attività premendo il tasto ⊞ (⌘ su Mac), poi scriviamo `remote`, clicchiamo su "Remote viewer". La prima volta, occorrerà indicare l'indirizzo della macchina virtuale dentro il campo "Connection address". Generalmente l'indirizzo è: `spice://localhost:5900`. Se stanno andando contemporaneamente varie macchine virtuali, la prima che si è avviata avrà come indirizzo `spice://localhost:5900`, la seconda `spice://localhost:5901` e così via. Dalla seconda volta in poi potremo cliccare sull'indirizzo desiderato dentro "Recent connections". Clicchiamo quindi sul tasto "Connect".

⚠ *Attenzione*: prima di selezionare la casella "Condividi cartella", dobbiamo essere molto sicuri di voler permettere al sistema Windows di leggere tutto il contenuto della cartella che stiamo condividendo.

Dentro la finestra del "Remote viewer" che contiene la macchina virtuale Windows, clicchiamo sul menu "File" → "Preferenze". Nella finestra che si aprirà selezioniamo con il pulsante a destra la cartella che vogliamo condividere. Per selezionare la cartella leggibile da Windows è necessario scegliere

"Altro..." nel menu a tendina. Selezioniamo la casella "Condividi cartella".

⚠ *Attenzione*: Selezioniamo sempre la casella "Solo lettura" a meno che non si vogliano far uscire dei file dal Windows virtuale, nel qual caso daremo un nome esplicito alla cartella tipo "Cartella dove Windows può scrivere".

Copiare i file

Dopo poco nella macchina virtuale Windows dovrebbe diventare accessibile il disco Z: dentro il Gestore dei file, accessibile da Risorse del computer (nelle versioni più nuove di Windows "Questo PC"). In caso contrario possiamo provare, nell'ordine, a fare queste tre cose:

- cliccare sul tasto refresh dentro il gestore dei file;
- chiudere e riaprire il gestore dei file;
- riavviare Windows.

Una volta riusciti a vedere il disco "Z", ovvero la cartella che abbiamo scelto di condividere, possiamo leggere tutti i file e le cartelle che contiene e copiare quello che ci interessa su un'altra cartella all'interno di Windows.

Interrompere la condivisione

Per una ragione o per l'altra, potremmo voler interrompere la condivisione della cartella con Windows.
Apriamo la vista d'insieme delle Attività premendo il tasto ⊞ (⌘ su Mac), poi scriviamo `remote`, clicchiamo su "Remote viewer". La prima volta, occorrerà indicare l'indirizzo della macchina virtuale dentro il campo "Connection address". Generalmente l'indirizzo è: `spice://localhost:5900`. Se stanno andando contemporaneamente varie macchine virtuali, la prima che si è avviata avrà come indirizzo `spice://lo-`

`calhost:5900`, la seconda `spice://localhost:5901` e così via. Dalla seconda volta in poi potremo cliccare sull'indirizzo desiderato dentro “Recent connections”. Clicchiamo quindi sul tasto “Connect”.
Dentro la finestra del “Remote viewer” che contiene la macchina virtuale Windows, clicchiamo sul menu “File” → “Preferenze”. Nella finestra che si apre deselezioniamo la casella “Condividi cartella” per la cartella che non vogliamo più condividere. La cartella selezionata adesso non sarà più accessibile da Windows.

23 | Aggiornare un sistema

Come abbiamo spiegato nel cap. 3.2, i malware si introducono di nascosto all'interno dei nostri computer grazie, tra le altre cose, a delle "falle di sicurezza".
Via via che questi errori di programmazione (o di progettazione) vengono scoperti, vengono regolarmente messe a disposizione delle correzioni. Quando sono disponibili è particolarmente importante sostituire le vecchie versioni dei software. Anche perché a quel punto i problemi corretti, che prima magari erano noti solo a qualche specialista, diventano palesi e riportati pubblicamente... e dunque diventa più facile sfruttarli.

23.1 Aggiornare Tails

I software evolvono, per questo è vivamente consigliato utilizzare la versione più aggiornata di questa ricetta, che troverete in francese e in italiano sui siti della Guida https://guide.boum.org/ e https://numerique.noblogs.org/.

Durata: da mezz'ora a un'ora, più circa un'altra mezz'ora per il download.

Essendo un sistema Live[1] una collezione indivisibile di programmi, eseguiti a partire da un DVD o da una penna USB, l'unico modo praticabile per utilizzare sempre le ultime versioni di questi programmi è quella di assicurarsi di stare usando l'ultima versione del sistema Live.
All'avvio di Tails, se ci sono aggiornamenti o una nuova versione disponibile viene mostrato un avviso per avvertirci che è di-

1 Cap. 14

sponibile una nuova versione che corregge le falle di sicurezza.
Nel caso in cui la stiamo utilizzando da DVD, bisogna distruggerlo e masterizzarne uno nuovo. A meno che non sia riscrivibile, nel qual caso basterà cancellarlo e rimasterizzarci sopra l'ultima versione di Tails.
Nel caso di una penna USB, e se disponiamo di una connessione a internet, possiamo direttamente usare l'utility Tails Upgrader. Basta cliccare su "Aggiorna adesso" e seguire le indicazioni. Se si verifica un errore, o se è necessario utilizzare un altro metodo di aggiornamento, l'utility ci guiderà verso la pagina giusta della documentazione, che si trova anche guardando nella Documentazione di Tails, sula Scrivania. Nel menu a destra clicchiamo su "Documentazione". Nell'indice che si apre cerchiamo la sezione "Primi passi con Tails" e clicchiamo sulla pagina "Aggiornare una penna USB o una scheda SD".

23.2 Aggiornare un sistema cifrato

Una volta installato[2], per poterci fare affidamento, un sistema cifrato deve essere mantenuto aggiornato. Le sezioni che seguono riguardano il sistema Debian, ma i concetti si applicano a grandi linee a quasi ogni altro sistema.
Il progetto Debian pubblica, più o meno ogni due anni, una versione *stabile*. Questo implica un enorme sforzo per coordinare la compatibilità tra le differenti versioni dei software, fare molti test e assicurarsi di eliminare i difetti più importanti.

23.3 Gli aggiornamenti quotidiani

↻ I software evolvono, per questo è vivamente consigliato

---

2 Cap. 15

utilizzare la versione più aggiornata di questa ricetta, che troverete in francese e in italiano sui siti della Guida https://guide.boum.org/ e https://numerique.noblogs.org/.

Durata: un minuto per lanciare l'aggiornamento, poi un tempo variabile per il download e l'installazione, durante il quali possiamo continuare a utilizzare il computer.

Il bello di una versione stabile di Debian è che, da quel momento in poi, i software che la compongono non verranno più modificati in profondità: verranno aggiunti soltanto miglioramenti alle traduzioni e correzioni a problemi legati alla sicurezza o che impediscono il normale funzionamento di un programma.
Queste nuove versioni possono quindi essere generalmente installate "ad occhi chiusi" e non dovrebbero perturbare le nostre piccole abitudini.
Se abbiamo installato l'*ambiente grafico*, il sistema verificherà in automatico, appena ci si connette a internet, la disponibilità di nuove versioni dentro ai repository che abbiamo configurato[3].
Quando è il caso, apparirà una notifica a indicarci che sono disponibili dei nuovi aggiornamenti.
Clicchiamo quindi sulla notifica, che apre il "Gestore degli aggiornamenti".
Verrà visualizzata una lista degli aggiornamenti. Clicchiamo su "Restart & install". Ci viene chiesta la password di amministrazione, diamogliela. In seguito confermiamo cliccando di nuovo su "Restart & install". Il computer si riavvierà e ci chiederà la passphrase di cifratura dell'hard-disk, sia prima di installare gli aggiornamenti, sia per ripartire poi sul nuovo sistema aggiornato.

3 Cap. 16.4

23.4 Passaggio ad una nuova versione stabile

I software evolvono, per questo è vivamente consigliato utilizzare la versione più aggiornata di questa ricetta, che troverete in francese e in italiano sui siti della Guida https://guide.boum.org/ e https://numerique.noblogs.org/.

Durata: da una mezza giornata a una giornata, di cui gran parte per il download (durante il quale possiamo continuare a utilizzare il computer) e un'altra buona parte per l'installazione (durante la quale è meglio non utilizzarlo).

Quando esce una nuova versione stabile di Debian, il progetto si occupa di mantenere gli aggiornamenti della precedente versione stabile, chiamata *oldstable*, per la durata di un anno[4]. Dobbiamo quindi approfittare di questo periodo di tempo per aggiornare il nostro sistema verso questa nuova versione. Si tratta di un processo più delicato rispetto all'aggiornamento quotidiano, non tanto per la realizzazione stessa, ma più per il fatto che poi sarà necessario adattarsi ai cambiamenti subiti dai programmi che usiamo abitualmente.

23.4.1 Passaggio da Jessie a Stretch

La procedura che spieghiamo qui di seguito riguarda il passaggio da una Debian chiamata *Jessie* o *8* (uscita nell'aprile del 2015), alla versione *Stretch* o *9* (uscita nel giugno del 2017)[5].

4 https://wiki.debian.org/it/DebianOldStable

5 Mentre scriviamo l'edizione italiana siamo nel luglio del 2020 e l'attuale versione stabile di Debian si chiama *Buster* o *10* ed è stata rilasciata nel luglio del 2019. Ciascun passaggio di versione ha le sue peculiarità ed è quindi impossibile generalizzare troppo. Queste ricette servono a dare delle nozioni di comprensione generale, che poi dovranno essere integrate e migliorate con l'esperienza diretta. [NdT].

Documentiamo qui una procedura semplificata per l'aggiornamento, che è stata testata su alcune installazioni di Debian Jessie con un ambiente grafico GNOME e dei software che provengono unicamente dai repository ufficiali Debian.
Per la durata dell'aggiornamento, è necessario avere a disposizione una connessione internet.

⚠ *Attenzione*: Questa procedura semplificata ha meno possibilità di funzionare se nel tempo abbiamo alterato il nostro sistema aggiungendo dei repository non ufficiali.

Se serve, possiamo fare riferimento alle note di rilascio ufficiali del progetto Debian, soprattutto nella parte "Aggiornamento da Debian 8 (Jessie)" e nella parte "Problemi di connessione per Stretch".

Aggiornare la nostra Debian Jessie
Prima di tutto è necessario disporre di una Debian Jessie aggiornata. Senza questo, il passaggio di versione rischia di non funzionare. Nel caso in cui non avessimo fatto gli aggiornamenti quotidianamente[6], è questo il momento di rimediare. Se ci viene proposto di riavviare il computer, in seguito a numerosi aggiornamenti, facciamolo prima di proseguire con il resto delle operazioni.

Assicurarsi di avere abbastanza spazio libero sull'hard-disk
Per evitare spiacevoli sorprese bisogna avere almeno 4 GB di spazio libero sull'hard-disk che contiene il sistema.
Apriamo la vista d'insieme delle Attività premendo il tasto ⊞ (⌘su Mac), poi scriviamo `fil` e clicchiamo su "Gestore dei file". Nella colonna di sinistra clicchiamo su Computer. Nel menu

6 Cap. 23.3

☰, scegliamo “Proprietà”. Nella finestra che si apre troveremo l’informazione che ci interessa.

Liberare spazio sul disco se necessario
Se non c’è abbastanza spazio libero sull’hard-disk, una soluzione è quella di cancellare le vecchie versioni degli aggiornamenti divenuti ormai obsoleti. Per farlo, apriamo la vista d’insieme delle Attività premendo il tasto ⊞ (⌘ su Mac), poi scriviamo `pacchett` e clicchiamo su “Gestore dei pacchetti”. Siccome il Gestore dei pacchetti consente di modificare il software installato sul computer, serve la password di amministrazione per aprirlo.
Nel menu “Impostazioni” scegliamo “Preferences”, poi selezioniamo la scheda “File” e clicchiamo sul pulsante “Elimina i pacchetti scaricati”, poi su “Applica” e poi chiudiamo il Gestore dei pacchetti Synaptic.
Verificare di nuovo lo spazio disco disponibile, come spiegato sopra. Se ancora non basta, occorrerà eliminare alcuni dei nostri file o disinstallare dei programmi.

Disattivare il salvaschermo
Durante l’aggiornamento, il salvaschermo potrebbe incepparsi e lasciare lo schermo bloccato. È più prudente quindi disattivarlo per il tempo dell’aggiornamento.
Per farlo apriamo la vista d’insieme delle Attività premendo il tasto ⊞ (⌘ su Mac), poi scriviamo `prefer` e clicchiamo su “Preferenze”.
Clicchiamo su “Salvaschermo”, nella finestra che si apre deselezioniamo l’opzione “Avviare” il salvaschermo quando il computer è inattivo. Chiudere la finestra e uscire dalle Preferenze.

Installare un software necessario alla procedura di aggiornamento
Per fare in modo che il nostro sistema cifrato possa chiederci

le domande legate all'aggiornamento tramite un'interfaccia grafica, bisogna installare il pacchetto[7] `python-glade2`.

Aggiornare i repository Debian

L'aggiornamento è testato soltanto per i pacchetti forniti ufficialmente da Debian Jessie. Dobbiamo quindi:

- da una parte, utilizzare i repository ufficiali della nuova versione stable;
- dall'altra, disattivare tutti gli altri repository Debian[8], compresi i backports.

Per farlo apriamo la vista d'insieme delle Attività premendo il tasto ⊞ (⌘ su Mac), poi scriviamo `pacchett` e clicchiamo su "Gestore dei pacchetti".
Dato che stiamo scegliendo i programmi su cui fare affidamento, dobbiamo inserire la password di amministrazione.
Nel menu "Impostazioni" scegliamo "Repository". Clicchiamo su una riga alla volta e:

- deselezioniamo tutti i repository con una URL non ufficiale (diversa da *debian.org*) e i repository backports;
- se nel campo Distribuzione c'è scritto "jessie", sostituiamolo con "stretch";
- se nel campo Distribuzione c'è scritto "jessie/updates o jessie-updates", rimpiazziamolo rispettivamente con "stretch/updates" o "stretch-updates".

Chiudiamo questa finestra cliccando su "OK" e aggiorniamo i reposotory cliccando su "Aggiorna".

7 Cap. 16.3
8 Cap. 16.4

Lanciare il passaggio di versione vero e proprio

Clicchiamo sul pulsante “Seleziona aggiornamenti”. Si aprirà una finestra intitolata “Selezionare le ulteriori modifiche richieste?”. Scegliamo “Seleziona”.
Lanciamo il passaggio di versione vero e proprio cliccando su “Applica”. Si aprirà una finestra intitolata “Applicare le seguenti modifiche?”. Dentro “Riepilogo”, possiamo verificare che viene previsto di aggiornare moltissimi pacchetti. Clicchiamo su “Apply”.
Il sistema inizierà allora a scaricare gli aggiornamenti da internet, il che potrebbe impiegare da qualche decina di minuti ad alcune ore, a seconda della velocità della nostra connessione.
Potrebbe aprirsi una finestra “Changelogs”. Mostra in inglese un elenco di cambiamenti importanti che saranno applicati. Clicchiamo su “Chiudi”.
La finestra “Installazione e rimozione dei software” mostra il procedere dell’aggiornamento.
Potrebbe comparire una finestra intitolata “Configuring libc6”. Scegliamo “Restart services during package upgrades without asking?” e poi clicchiamo su “Forward”.
Potrebbe comparire anche una finestra “Synaptic”. Indica che un file di configurazione è stato modificato e ci chiede se vogliamo sostituirlo con la sua nuova versione. “Mantenere” o “Sostituire” è una scelta che dipende dall’importanza delle modifiche che abbiamo potuto apportargli rispetto alle novità proposte. Non esiste quindi una risposta genericamente valida. Bisogna comparare le versioni oppure tirare a indovinare.
Una volta finito l’aggiornamento, viene mostrata una finestra intitolata “Le modifiche sono state applicate”. Clicchiamo su “Chiudi” per chiudere il Gestore dei pacchetti.

Primo riavvio

È venuto il momento di riavviare il sistema, utilizzando il menu in alto a sinistra e scegliendo “Riavvia”.

Riabilitare i repository Debian supplementari
Possiamo riprendere fiato. Il grosso è fatto. Restano ancora solo alcuni piccoli aggiustamenti...
Se abbiamo disattivato i repository non ufficiali prima dell'aggiornamento, è il momento di verificare che con la nuova versione di Debian ne abbiamo ancora bisogno. Se sì, riattiviamoli[9]. Allo stesso modo possiamo riattivare il salvaschermo.

Riattivare il salvaschermo
Apriamo la vista d'insieme delle Attività premendo il tasto ⊞ (⌘ su Mac), poi scriviamo `prefer` e clicchiamo su "Preferenze".
Clicchiamo su "Salvaschermo", nella finestra che si apre selezioniamo l'opzione "Avviare il salvaschermo quando il computer è inattivo". Chiudere la finestra e uscire dalle "Preferenze".

Assicurarsi che il nuovo sistema funzioni correttamente
Potrebbe essere utile assicurarsi che le azioni e i comandi più ricorrenti funzionino bene. Eventualmente potrebbe dover essere necessario diagnosticare e risolvere alcuni problemi. È sicuramente meglio prendere confidenza con il nuovo sistema, in modo da poter convivere per i prossimi due anni con un sistema funzionante.
I problemi più frequenti vengono spesso descritti, con i trucchi per risolverli, all'interno della diversa documentazione che riguarda Debian e GNU/Linux[10].
Ricordiamoci anche che esistono le note di rilascio ufficiali del progetto Debian.

9 Cap. 16.4
10 Cap. 15.7

24 | Ripulire i metadati di un documento

I software evolvono, per questo è vivamente consigliato utilizzare la versione più aggiornata di questa ricetta, che troverete in francese e in italiano sui siti della Guida https://guide.boum.org/ e https://numerique.noblogs.org/.

Durata: qualche minuto.

Lo scopo di questa ricetta è quello di cancellare i metadati presenti all'interno di un documento[1] prima di renderlo pubblico. Questi metadati non sono gli stessi per ogni formato di documento: alcuni sono più difficili da ripulire, persino impossibili. Nonostante ciò la maggior parte dei formati utilizzati per scambiarsi dei documenti finiti, siano testi, immagini, audio o video, sono "ripulibili".
Lo strumento che useremo si chiama *Metadata Anonymisation Toolkit* (MAT), e permette di ripulire facilmente molti formati di file.

Attenzione: Ripulire i metadati non anonimizza il contenuto dei file, e non rimuove eventuali marchi[2] che potrebbero essere inclusi nel contenuto stesso.

24.1 Installare il software necessario

In Tails, Metadata Anonymisation Toolkit è già installato. In un sistema dove il pacchetto non è ancora presente, bisogna installarlo[3].

---

1 Cap. 2.6
2 Riguardo a questo: http://dadefi.vado.li/ e http://polozu.vado.li/.
3 Cap. 16.3

24.2 Aprire Metadata Anonymisation Toolkit

Apriamo MAT partendo dalla vista d'insieme delle Attività: premiamo il tasto ⊞ (⌘ su Mac), poi scriviamo `mat` e clicchiamo su "MAT".

24.3 Aggiungere dei file da ripulire

Aggiungiamo il file da ripulire cliccando sul pulsante "Add". Selezioniamo il file e clicchiamo su "OK". Possiamo anche trascinarlo direttamente dentro Metadata Anonymisation Toolkit. Si possono anche aggiungere più file e ripulirli nello stesso momento. Se il software è in grado di ripulire il file selezionato lo aggiunge alla lista dei file da ripulire. Passiamo dunque al paragrafo dopo.
Se compare un messaggio "Non supportato", bisogna prima convertire il documento in un formato di file supportato da MAT. La lista dei formati supportati è disponibile cliccando su "Help" → "Info".
Spesso si tratta di esportarlo in un comune formato di condivisione. Per esempio MAT non è in grado di ripulire i file xcf del programma di manipolazione delle immagini GIMP, ma può ripulire le immagini esportate in formato jpeg o png.

24.4 Ripulire i file

Una volta aggiunto il file, ripuliamolo cliccando sul pulsante "Clear". A questo punto possiamo chiudere Metadata Anonymisation Toolkit.

INDICE

III. Utensili